An Implementation Strategy for Bring Your Own Device in the NHS: An Innovation Study

by

Rob Blagden

A Master's Dissertation Proposal Presented to the
FACULTY OF THE MSc in DIGITAL HEALTH LEADERSHIP
THE INSTITUTE OF GLOBAL HEALTH INNOVATION
IMPERIAL COLLEGE LONDON
In Partial Fulfilment of the
Requirements for the Degree
Master of Science in Digital Health Leadership

Date: 22nd March 2020

 01568418

Dedication

This research study is dedicated to the memory of

Carol Margaret Blagden.

A brilliant mother who always encouraged me

to keep learning new things

and to find the good in every circumstance.

Acknowledgements

This research would not have been possible without the time and input from those who contributed to surveys and interviews. The support of Imperial College faculty and NHS Digital Academy colleagues has also been invaluable. I couldn't have got here without Rachael Dunscombe and others believing in me. Thanks to Ruth Claire Black for inspiring this topic and for the ongoing advice and guidance that kept me focused and motivated. The honest feedback and frequent encouragement from my wonderful peer group colleagues has been fantastic, we are #TBFL. A huge thank you to everyone who has helped to make this research a reality. A special thank you to my wife Joybelle and my amazing family for giving me the space and time to study – you are my everything. Finally thank you to my anonymous kidney donor and their family who chose to give me life in their most difficult moment. I could never have taken on this work without the freedom of a working kidney and body. They say #datasaveslives but so do #organdonors, these are the magnificent heroes in our society who do what technology cannot.

Table of Contents

List of Tables

List of Figures

Abstract

Little research has been completed in respect of Bring Your Own Device (BYOD) in the UK healthcare market. This study investigated how NHS staff and organisations feel about using their own devices for work tasks and whether there are key implementation processes that can be used to improve adoption and project success. Research evidences many benefits of BYOD including productivity, innovation, flexibility and increased attractiveness for the organisation in the areas of recruitment and retention. There is a desire amongst staff to use BYOD although this is muted in clinical roles where concerns are significant about data security and work / life balance. Policies in organisations offering BYOD are often ambiguous, user unfriendly, difficult to find or simply don't exist and this should be addressed to protect people and valuable data assets. This policy inadequacy is not unique to the NHS but is pervasive in the wider public sector. There is no standard implementation methodology for BYOD in every NHS organisation, however there are consistent themes relating to real engagement, policy clarity and monitoring which will benefit a wide range of BYOD projects if given adequate focus.

Key Words

NHS, BYOD, CYOD, CHANGE, CONSUMERISATION, DATA, DEVICE, DIGITAL, ENGAGEMENT, GOVERNANCE, HEALTH, IMPLEMENTATION, INNOVATION, LEADERSHIP, MANAGEMENT, MDM, MOBILE, MONITORING, PERSONAL, POLICY, SECURITY, SMARTPHONE, TECHNOLOGY

Chapter One: Introduction

Introduction of the Problem of Practice

Much has been written about Bring Your Own Device (BYOD) from a private sector perspective, but there is no specific guidance about the benefits and risks of BYOD in relation to the UK healthcare market. Where BYOD is in use in the NHS, there is wide variation from organisation to organisation in policy, uptake and approach. A recent study of a US hospital evidenced an unclear understanding of mobile device policies and what they permit (Stephens et al., 2017). A review is needed of existing NHS BYOD usage, the benefits and risks of BYOD and the development of best practice for BYOD implementation within the NHS System (Hallet and Aspinall, 2017).

Organisational Context and Mission

2gether NHS Foundation Trust (2gether) provides specialist mental health and learning disability services to the people of Gloucestershire and Herefordshire, serving a combined population of 780,461 with its 2,300 dedicated staff. 2gether is an innovative and forward-thinking organisation, with a deep commitment to providing a high-quality service in the local community. Rated 'good' overall (Care Quality Commission, 2018) 2gether is the first trust in the country to be awarded an 'outstanding' rating for acute inpatient services, crisis services and psychiatric intensive care services (2gether, 2019a). 2gether's vision is to be the provider and employer of choice providing high quality, cost-effective services. Key organisational priorities are: continuous quality improvement, internal and external engagement and transformation to ensure sustainability (2gether, 2019b).

Organisational Performance Status

2gether currently offers laptops as the default computing device although 10% of staff use standard desktop PCs. All laptops have remote working capability. Dependant on their role, community staff and managers are issued with mobile phones or smartphones. Most computers and mobile phones are over four years old and approaching end of life. Some senior leaders use NHSmail email on personal devices. While organisational mobile working policies allow this, there is no documented approach to BYOD. A Mobile Device Management (MDM) solution called Airwatch secures organisation owned smartphones and tablets but it is not used to control personal devices.

There is a desire to utilise BYOD because it can offer flexibility in support of the organisation's vision. However, there is a need to clearly understand the key components of the cost, risk and benefit of a BYOD programme. The Trust's 'can do' organisational culture results in the adoption of many different solutions and causes a level of confusion when users see an inconsistent interpretation of the rules and policies. This lack of clarity has resulted in an inconsistent approach to devices which increases the cost of support. Standards and core guidance are needed to describe various models of BYOD. Key elements of this study will include: How attractive is BYOD for clinical staff? What should be allowed under a BYOD policy? And, how is BYOD supported through policy and procedures? With clear and simple definitions of BYOD, the organisation will be equipped to make an informed decision on an approach that is appropriate, affordable and consistent.

Importance of the Organisational Innovation

It is important for the organisation to manage BYOD for a variety of reasons. These can be categorised as shown in Table 1 below. The priority placed on these will be different for users, the organisation and the technical support teams, but all have the potential to add value to the organisation as a whole. In 2gether, as with much of the NHS, workforce recruitment and retention is challenging, but essential to maintain continuity of services. Studies show that offering BYOD has a positive impact on retention, efficiency and adds to staff feeling valued and appreciated by the organisation.

User choice	Allowing self-selection of the type of device adds value to employees by demonstrating their needs and preferences are valued – this adds to a sense of worth and belief at an individual level which will improve commitment to the organisation (Capgemini Consulting. 2017).
Workforce retention	The literature confirms that BYOD supports the workforce in feeling valued and trusted. This creates a reason to stay which supports the goal of increased retention of staff and becoming an employer of choice (Weeger, A., Wang, X, Gerald, H., 2015).
Efficiency	When staff can use their own devices, they are more productive because they are working in an environment tailored to them. There are also indications in the literature that staff may become more innovative when allowed to work on their own device (Bresnick, 2013).
Support cost	Supporting a user on their own device is cheaper because they are familiar with its use and are responsible for maintaining it. This increases reliability and reduces the overall cost of support (Mahindru, 2013).
Environment	Having a computer at home and at work and a mobile phone for work and another for personal use does not represent a responsible approach to the use of the finite resources needed to manufacture electronic systems (Oaks, 2013).

Table 1. *Reasons to introduce BYOD into the organisation.*

Without clarity on the best approach to BYOD, the organisation risks having a chaotic and unmanaged environment where data could be put at risk inadvertently. Without clear policies and boundaries some staff may choose to use their own device without appropriate thought given to information security. The Trust has a duty of care to protect data and support clinicians in having appropriate knowledge of how to access information securely.

Organisational Performance Goal

There are staff within the organisation who desire increased flexibility to use their own personal computing devices for work-related communication. The organisation is keen to be responsive to user requests by leading a culture which supports digital innovations that improve service quality, organisation sustainability and user choice. The Trust needs to understand how BYOD can impact organisation performance goals. Evidence from this study will provide intelligence on user perspectives regarding BYOD and whether it offers a viable improvement to the current model.

Stakeholder Group for the Study

The stakeholder group will include community clinicians as they are a key beneficiary of the BYOD solution. Gaining their user perspective will increase programme support and success (Pagliari, 2007). Other stakeholder groups will include external organisations and technical teams. This study will aim to understand user needs and technical challenges, contributing towards a body of knowledge that can improve BYOD implementation.

Research Question

The question that will guide this study is: Do the benefits of implementing Bring Your Own Device (BYOD) in UK healthcare market outweigh the potential risks, and is there an optimum implementation methodology that NHS trusts should follow?

Methodological Framework

This project will employ mixed method data gathering and analysis. The stakeholder's current perspectives on BYOD will be assessed through surveys and interviews and compared to a control group of other organisations. External NHS employees will be asked to complete surveys including a

user survey and a technical survey which aims to discover implementation experience. Technical BYOD experience will be gathered using surveys, interviews, Freedom of Information (FOI) requests and a document review of existing BYOD policies. BYOD implementation advice and a template example policy will be developed and recommended based on this research.

CHAPTER TWO: REVIEW OF THE LITERATURE

At 2gether there is a commitment to make use of the flexibility offered by BYOD. However, the organisation has no documented approach. Academic papers regarding the use of BYOD, specific to UK healthcare, are limited, and there is an absence of documented and tested best practices, strategies and approaches to implementing BYOD in the NHS.

Literature Related to the Problem of Practice

In the private sector there is much discussion about BYOD and the opportunity and risk that it introduces. Yet, within UK healthcare context there is little specific literature. BYOD does not appear to have been discussed widely.

Policy Guidance

National policies exist but are generic and were created before GDPR compliance became a requirement. Central NHS guidance comes from an NHS Digital example BYOD policy (NHS Digital, 2017a) which is limited and dependant on an Acceptable Use Policy (NHS Digital, 2017b). Risk in the NHS is a local trust responsibility and this can cause variation in how BYOD solutions are considered and implemented. The inconsistent use of BYOD can be confusing for staff and adds risk as people transition between employers who have completely different approaches.

Hallet and Aspinal (2017) review common concerns in BYOD policies and highlight a variety of styles and approaches. Some policies are prescriptive, explicitly defining what is and is not permissible. Other policies are based on a contract with the user, requiring acknowledgement of company defined rules and agreement to follow them. Contract-based policies are useful because they allow future needs to be covered in overarching compliance themes. Regardless of policy approach, many organisations propose use of Mobile Device Management (MDM) to protect confidential data because there is no perfect policy when BYOD usage is incongruous.

Benefits of BYOD include improved productivity, reduced costs, employee satisfaction, and increased flexibility. These benefits need to be balanced against the risks to organisation information, higher network usage, rapid pace of change, allowing untrusted devices and apps, increased support workload for IT departments, and unclear funding responsibilities (Varbanov, 2014).

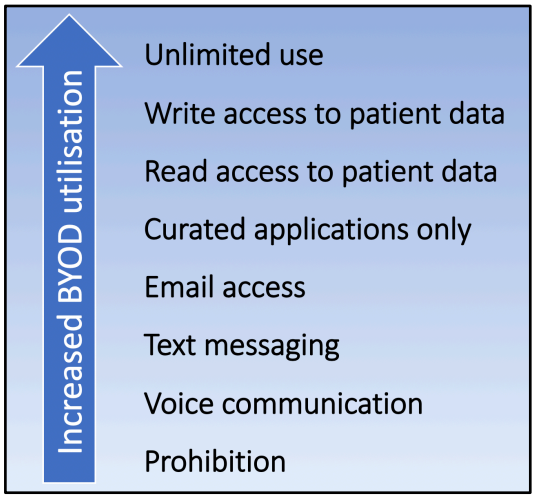


Figure 1. *Levels of BYOD Utilisation.*

As illustrated in Figure 1 above, approaches to BYOD can be ranked from prohibition to unlimited use and these reflect the level of trust an organisation is willing to place in systems and people.

Varbanov (2014) proposes several steps to implementing BYOD which can be summarised as:

1. Understanding organisation/employee requirements
2. Identifying risks
3. Discussion of technologies that could be used
4. Creating rules for participation
5. Implementation

Though not NHS centric, Varbanov's approach is sensible. There is a consistent theme in the literature suggesting that a corporate BYOD strategy and policy is essential. Absence of a policy leaves organisations open to personal definition, unmanaged risk, and potential staff abuse.

Consumerisation Trends

A 2015 report in the Journal of Information Systems (Weeger, Wang and Gerald, 2015) discussed changes in consumer adoption of personal computers and smartphones. Usage has increased as usability and style has made technology more attractive to use and own. As a result, employees are more comfortable with personal devices than corporate devices, which often have not kept pace with the rapid evolution in the home retail market. The article concluded that people increasingly use lots of different kinds of mobile devices and strongly expect to use personal devices for work purposes and this causes them to prefer employers who are offering a BYOD program. Additionally, the future

workforce (who have grown up with mobile devices) have strong expectations that employers will allow them to use personal devices at work.

Familiarity with technology in personal life is a driver for the adoption of BYOD at work. It is increasingly difficult for organisations to prevent employees from using personal devices to fulfil business tasks (Leventhal, 2017). Further, there are surveys that find a majority of doctors use personal smartphones to share patient data using WhatsApp (Digital Health, 2018). BYOD is cited as improving employee motivation and potentially increasing autonomy and performance (Doargajudhur and Dell, 2018). As stated by Mitrovic et al. (2014): 'BYOD is a reaction to a rising demand from employees and can be strategically used to preserve or attract the most talented employees – the workforce of the future.'

Köffer, Ortbach and Niehaves (2014) investigate the relationship between IT consumerisation and job performance. The research concludes that consumer IT facilitates the electronic integration of a person's work and personal life because they can use the same hardware and software for both their private and work tasks. People enjoy using consumer IT because of the advanced features offered and because it is their own. There is a question on how much work-life integration employees need or want as this is not explored in the literature. In the NHS a clear understanding is required on what acceptable use means if a personal device can access patient data alongside private apps.

In healthcare, where data is highly sensitive in nature, there is concern about how to balance privacy and security. This is understandable given regular reports of hacking and data breaches (Lee, 2019). However, rather than resisting BYOD, organisations should embrace and manage it to avoid the chaos of data being completely uncontrolled (Cidon, 2015). The provision of a standardised BYOD implementation toolkit specific to health would provide IT managers increased confidence in their solution configuration.

Goodhue and Thompson (1995) suggest that technology is likely to be more 'task fit' if users are involved in the design and testing process when new technology is being evaluated. In an NHS organisation where there are hundreds of different roles and thousands of staff each with unique abilities and competencies it is impossible to provide a one-to-one technology choice that is perfect for all. Enterprise technology generally takes a one size fits all utility approach. The personalisation

BYOD offers can increase performance by combining consideration for how people prefer to use systems with the tasks they need to complete.

Personally-owned devices are more likely to be modern than NHS-issued devices, many personal devices are under 800 days old (Chen, 2013). BYOD allows the user to download a range of applications and utilise them in the workplace, subject to policy limitations. In comparison, the ability to test different software solutions is not afforded on centrally managed organisation devices. Personal devices may also include cameras, microphones and other technology which seamlessly integrates into applications and software. The challenge for the organisation is how to police an explosion in software and data and how to ensure it is accredited for use in a medical environment. MDM software does allow organisations to limit software to a curated list of applications within the work context and BYOD policies need to factor in a process for users to request updates to this approved list.

Efficiency Incentives

Another key challenge is understanding how cost savings materialise. In savings analysis of BYOD there are reports of an average saving per employee of 81 minutes per week (Chen, 2013). Other potential savings opportunities are listed in Table 2 below.

BYOD Savings
Increased employee productivity
Reduction in device costs for organisation
Reduction in training time for new employees
Reduced IT support and maintenance cost
Benefit of increased creativity afforded by newer technology

Table 2. *Savings opportunities from BYOD.*

BYOD increases productivity and innovation among workers and research shows employees prefer using their own device, increasing employee satisfaction and happiness (Chen, 2013). The savings generated are immediately offset by the cost of policing BYOD and securing organisation systems, see Table 3 below. On the question of does the saving outweigh the cost, the literature is split. Technology vendors suggest large savings on hardware, support and mobile contracts (Chen, 2013) but investigations reveal these are often based on idealistic scenarios and non-cashable

productivity benefits (Ackerman, 2018). Each scenario is unique and will require local interpretation and modelling based the proposed implementation.

BYOD Costs	
	BYOD software licenses
	BYOD device administration resource
	BYOD policy development, management and auditing
	Potential increased expense claims and cost of administrating such

Table 3. *Increased expenditure due to BYOD.*

Another difficult issue is staff compensation. There is no standard practice for employee reimbursement if they use their own device. NHS Digital stands alone in the NHS in offering employees a monthly contribution toward smartphone contracts to cover personal expenses. There is a lack of research around employee views on compensation versus benefit. Only about half of private sector BYOD programmes compensate via expenses or a stipend (Kanaracus, 2013). The reports reviewed do not discuss the NHS and therefore are not representative. It will be useful to review the perspective of NHS staff groups on the issue of who pays for BYOD versus who benefits.

Leadership

On the subject of leadership there is evidence that organisations are slow to adopt digital change even though it has become an imperative. Whilst the need for digital transformation is recognised many say their leaders lack urgency, vision and focus on key digital transformation issues (Fitzgerald et al., 2013). The Embracing Digital Change survey findings (Figure 2) demonstrate the need for the full support of the board to promote digital change initiatives (such as BYOD) as organisational change programmes rather than IT projects.

The Digital Transformation Compass (DTC) is a tool to develop and sustain digital leadership and engagement in an organisation (Figure 3). The concepts in DTC provide a structure to take users and senior leadership on the digital change journey which requires a fusing of the business and IT leadership to successfully drive the transformation programme (Westerman, Bonnet and McAfee, 2014). Involvement of executives, Human Resources, doctors, clinicians and technologists in policy implementation will ensure it is created via a two-way dialogue where the real concerns and needs of users are listened to and reflected in the output. In past technology implementations, the NHS has not

engaged meaningfully (e.g. The National Program for IT) and this has resulted in resistance to change. Understanding concerns from users and board members will be important in a BYOD implementation. The approach of the DTC can be used to help guide development of the BYOD implementation strategy.

- According to 78% of respondents, achieving digital transformation will become critical to their organizations within the next two years.
- 63% said the pace of technology change in their organization is too slow.
- The most frequently cited obstacle to digital transformation was "lack of urgency."
- Only 38% of respondents said that digital transformation was a permanent fixture on their CEO's agenda.
- Where CEOs have shared their vision for digital transformation, 93% of employees feel that it is the right thing for the organization. But, a mere 36% of CEOs have shared such a vision.

Figure 2. *Key findings from the "Embracing digital change" survey (Fitzgerald et al., 2013).*

Figure 3. *The Digital Transformation Compass (Westerman, Bonnet and McAfee, 2014).*

Literature Linking the Project to National Programmes

BYOD literature specific to the NHS is limited. However, there are a plethora of US-based studies. One such example is a review of a US healthcare facility where BYOD was encouraged to facilitate communication between teams. There was evidence suggesting communication improved. However, the response was mixed with some users saying at times BYOD became a distraction due to increased interruptions leading to heightened perceptions of overload. The review investigated the impact on boundaries between personal, work, and different teams. Some staff were 'segregators' and wanted to keep personal and work communication separate, whereas those termed 'integrators' were quick to adopt and manage the different communication needs from a single device. The report highlighted differences in roles, citing doctors as having more freedom to choose how to use personal devices, whereas nurses operate in a more hierarchical job role which impacted adoption and acceptance. At times adoption of BYOD was impacted because policy legacy confused users about what was and was not permissible (Stephens et al., 2017).

The review discussed other issues such as user willingness to allow organisation MDM control of personal devices and who bears the cost of using the device in a work context. The report concluded that an individual's perception of their role can impact adoption of BYOD and therefore organisations should take a flexible approach to deployment that considers roles, attitudes and needs. (Stephens et al., 2017). This is a useful paper but it has limitations as it only looks at the use of BYOD for communication and does not investigate use of apps or access to patient data.

The NHS Long Term Plan has goals to expedite novel innovation to deliver improved care from new treatments and technology (NHS England, 2019a). BYOD is an innovation that has potential to deliver significant benefit if implemented well. One influencer of successful adoption of BYOD is diffusion of innovation theory. (Meske et al., 2017). This can help explain variable adoption rates based on the type of user and role. Innovators often want independence regardless of policy, but the late majority and laggards will need more structure to embrace the new BYOD model. This presents a challenge and suggests a multi-level policy may be needed to accommodate the needs of different users. This reinforces the need for top level leadership of BYOD implementation programmes and appropriately thought through policies.

There are several challenges posed by BYOD in healthcare. One challenge is the management of user-owned devices. In a majority of corporate networks, including the NHS, adding devices to the network is under the sole control of the IT Department. Education is needed to help technical staff understand the risk of the new model in proportion to the benefit perceived by the organisation. Security controls increasingly need to shift away from managing devices at a micro level to focusing on securing and managing enterprise applications and their data (Williams, 2014).

Recent NHS policy and publications propose that the NHS moves to a consistent approach to technology which is based on using open standards. (Department of Health & Social Care, 2018). This vision suggests utilising the internet rather than dedicated NHS networks to make connectivity more affordable (NHS Digital, 2019). It also mandates that future NHS software should operate in any web browser from any device and that systems are cloud-hosted. This aspirational operating model for NHS technology is an ideal environment for BYOD solutions.

Conclusion

'BYOD is not a simple IT project. It questions how IT is viewed and implemented, and requires significant evolution in IT organisation to promote service-oriented models' (Capgemini Consulting, 2013).

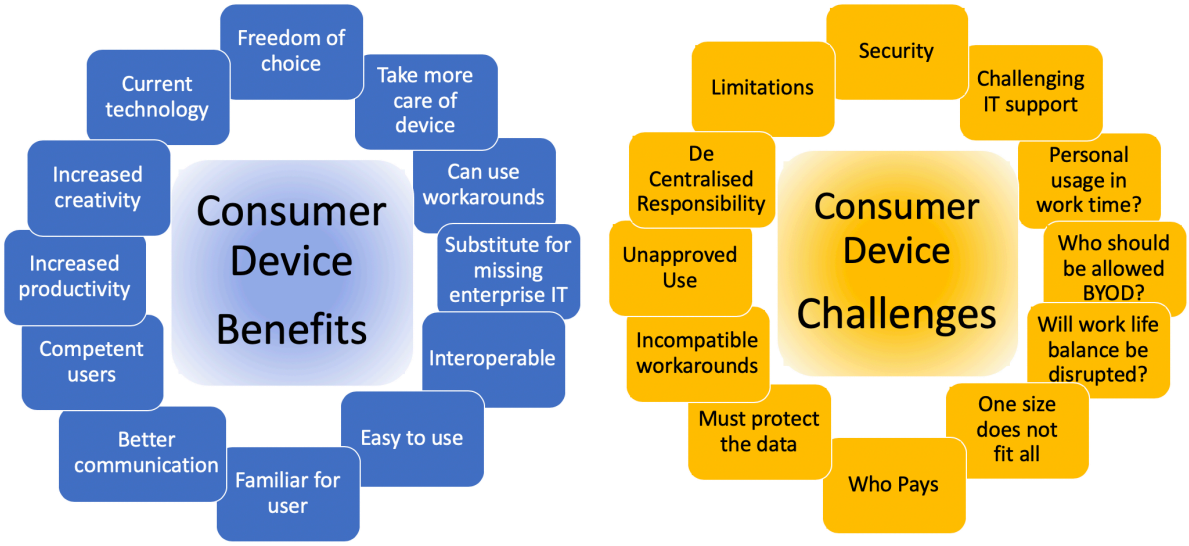


Figure 4. *Benefits and challenges of BYOD.*

BYOD provides demonstrable benefits when implemented with clear strategies and supporting policies. Staff adoption is variable and this is impacted by a variety of factors such as communication style, employee role and willingness to blur the traditional boundaries between

personal and work life. There are links to increased productivity and workforce retention which are key drivers for implementation although this is not widely evidenced in NHS clinical roles.

Moving to a standardised implementation approach will ensure security concerns are adequately addressed and offers an opportunity for consistency between organisations in addressing key challenges and exploiting exciting opportunities shown in Figure 4. Organisations who do not wish to support BYOD should still discuss it and formally document their decision. In not addressing BYOD at all organisations leave themselves at risk of staff self-approving methods of work which may present future issues and risks.

CHAPTER THREE: METHODS

This chapter presents the methodological framework and methods for data collection. The question the research and data seek to answer is 'Do the benefits of implementing Bring Your Own Device (BYOD) in the UK healthcare market outweigh the potential risks and is there an optimum implementation methodology that NHS trusts should follow?'

Population of Study

Population 1: Clinical staff who operate from a range of locations and who may benefit the most from the flexibility of using BYOD.

A focus of this study will be NHS clinical staff employed by 2gether who work in the community. The reason for this selected population is due to the high potential for a peripatetic workforce to benefit from access to work resources outside of the office on their personal mobile device. The study aims to research the benefits and risks of BYOD and it will be useful to understand perspectives at the clinical end of workforce as the attitudes of this group have not been studied previously. For instance, do millennials expect BYOD to be available and does it make the employer more attractive? Do older workforce members have similar desires for BYOD? How does each cohort view the benefits versus risks? How does these views compare with technical teams? The study is related to 2gether but responses from external organisations will be sought to provide a comparator of views from a wider population.

Population 2: NHS Technical support staff who have a responsibility for maintaining computer systems and data security.

IT departments have significant influence over the use of BYOD because they need to provide support for users. BYOD increases the number of unmanaged devices in use generating a need for different tools and policies. The study will aim to understand technical issues and risks with BYOD implementation. The study will also explore the opinion of participants for and against BYOD and their reasoning. For organisations who have implemented BYOD the study will investigate their approach, permitted use, deployment volume and impact on support. For organisations who don't offer BYOD the study will investigate barriers that exist.

Population 3: Public sector organisations

In order to compare usage of BYOD in the NHS with other organisations the study will contact a range of public sector organisations to gather policies and positions on BYOD.

Population	Objective Summary
1: Community based clinical staff	To understand if users believe BYOD would deliver benefits in day to day work.
2: Technical support staff	To understand the impact of implementing and supporting BYOD.
3: Public sector organisations	To understand penetration of BYOD and whether organisations have supporting policies.

Table 4. *Population study objectives summary.*

Survey Sampling Criteria and Rationale

Method #1: User survey

Criterion 1: Anyone following the author of this study on Twitter.

Format: Single question delivering using Twitter's built-in poll feature.

Rationale: This sample from a wide audience will be compared with the more detailed survey results to see if at a high level the aspirations of using BYOD in the NHS are broadly in line with external perspective.

Proposed question: "Should employees be able to use their personal devices for work tasks?" Four possible answer options: Yes, Yes for some tasks, No, Don't know.

Outcomes: When the survey closes results will be published on Twitter and LinkedIn with information about the full survey (Criterion 2) to engage and draw readers into the main survey.

Criterion 2: Healthcare providers including NHS, social care and third sector organisations.

Format: Online survey asking for views from NHS, social care and third sector health care organisations on the subject of BYOD. Advertised via Twitter, LinkedIn and via direct email invitation.

Rationale: This sample will gather a base population against which 2gether's responses can be compared.

Proposed questions: Questions will include subjects such as "What do you think of BYOD?", "Do you use it?", "What task would you like to use BYOD for?", "Is it a benefit?", "Should your costs be covered?" The survey will collect some demographical information about responders.

Outcomes: Responses will be analysed and compared against those gathered via Criterion 3. A selection of respondents who indicate they are willing to take part in interviews will be contacted for follow up.

Criterion 3: Clinicians working for 2gether.

Format: Online survey asking for views on the subject of BYOD. Advertised via Twitter, LinkedIn and via direct email invitation.

Rationale: This criterion will enable understanding of the perceived benefits of BYOD within the patient-facing workforce. The survey will aim to discover whether there is an appetite for BYOD because user engagement will be critical to implementation success. The user perspective is likely to influence the optimum implementation methodology.

Proposed questions: as per Criterion 2.

Outcomes: Responses will be analysed and compared against those gathered via Criterion 2. A selection of respondents will be contacted for follow up interviews.

Method #2: Technical Survey

Criterion 4: Technical staff working across the NHS.

Format: Online survey asking for views on BYOD implementation and policy approach, advertised via Twitter, LinkedIn and via direct email invitation.

Rationale: This criterion will enable understanding of the implementation approach taken by other organisations and provide information regarding the impact on the provision of IT Support services caused by BYOD.

Proposed questions: Questions should include subjects such as “Does your organisation limit what can be accessed via BYOD?”, “Does BYOD generate increased IT support requirements?” , “Do you have a BYOD audit process to ensure policy is adhered to?”, “How would you rate risks in relation to BYOD?”, “What approach to BYOD implementation did your organisation take?” The survey will also need to collect some demographical information about responders.

Outcomes: These responses will help to form best practices for implementation and support answering the question “Is there an optimum BYOD implementation methodology for the NHS?”

Method #3: Public sector organisation survey

Criterion 5: A range of public sector organisations including NHS Trusts and CCGs

Format: Short Freedom Of Information (FOI) survey that encourages closed answers to facilitate data comparison and group organisations by whether they use BYOD and whether they have a policy to support it.

Rationale: This criterion will gather information on support for BYOD at an organisational rather than individual level. It will aim to gather policies from respondents. Sending the same queries to non-NHS organisation will provide a benchmark with which to compare the NHS.

Proposed questions: Questions will be kept to a minimum but will include "Does your organisation allow staff to use their own devices to access work email?" and "Does your organisation have a policy that covers BYOD or the use of personal devices at work?"

Outcomes: Responses will provide insight into how BYOD is implemented in a variety of organisations and contribute to understanding of best practices for implementation and support answering the question "Is there an optimum BYOD implementation methodology for the NHS?" Policies gathered will feed into the document review.

Survey Sampling Recruitment Strategy and Rationale

The research will aim for a total of 900 responses across surveys with 150 responses from Criterion 1 and 150 from Criterion 2 as a control group. 50 specific responses from 2gether will be sought in Criterion 3 to enable comparison of the perspectives towards BYOD in 2gether. For the technical survey (Criterion 4) the target is 50 responses. The public sector survey for Criterion 5 will be via a Freedom of Information Request (FOI) aiming for over 500 responses. It is estimated these numbers will result in sufficient sampling to enable achievement of saturation and redundancy in response variation (Lincoln & Guba, 1985).

In addition to sharing survey information online and within 2gether, some key contacts will be engaged to assist with recruitment to a wider audience using existing networks including Digital Academy colleagues, 2gether executives, CIO/CCIOs and Digital Health Networks.

Criterion	Objective Summary	Response Period	Response Target
1: Anyone who sees Twitter poll	To generate interest in the BYOD topic and provide opportunity to invite additional respondents for user and technical survey.	48 hours	150
2: Staff working for healthcare providers including NHS, social care and 3rd sector	User survey aiming to understand current feelings towards BYOD in general health care population.	4 weeks	150
3. Clinicians working for 2gether	User survey aiming to understand current feelings towards BYOD specific to 2gether.	4 weeks	50
4. Technical staff working across the NHS	Technical survey aiming to understand impact of BYOD within IT support side of NHS organisations.	4 weeks	50
5. Range of public sector organisations including NHS, councils and universities	Organisation survey focusing on use and policy provision.	20 working days	500

Table 5. *Criterion summary for study surveys.*

To gain as many responses as possible an online survey is the preferred method (Figure 5) because it will allow input from a wide geography allowing a greater scale of data to be collected (Merriam & Tisdell, 2016). The survey will be kept simple and questions will not be numbered so as not to distract respondents. The survey will be tested on a computer, smartphone and tablet to ensure it displays questions correctly. Questions will be limited to maximise the potential for full completion. Survey respondents will be offered the studies final output report and asked to consider engaging with the future interview process.

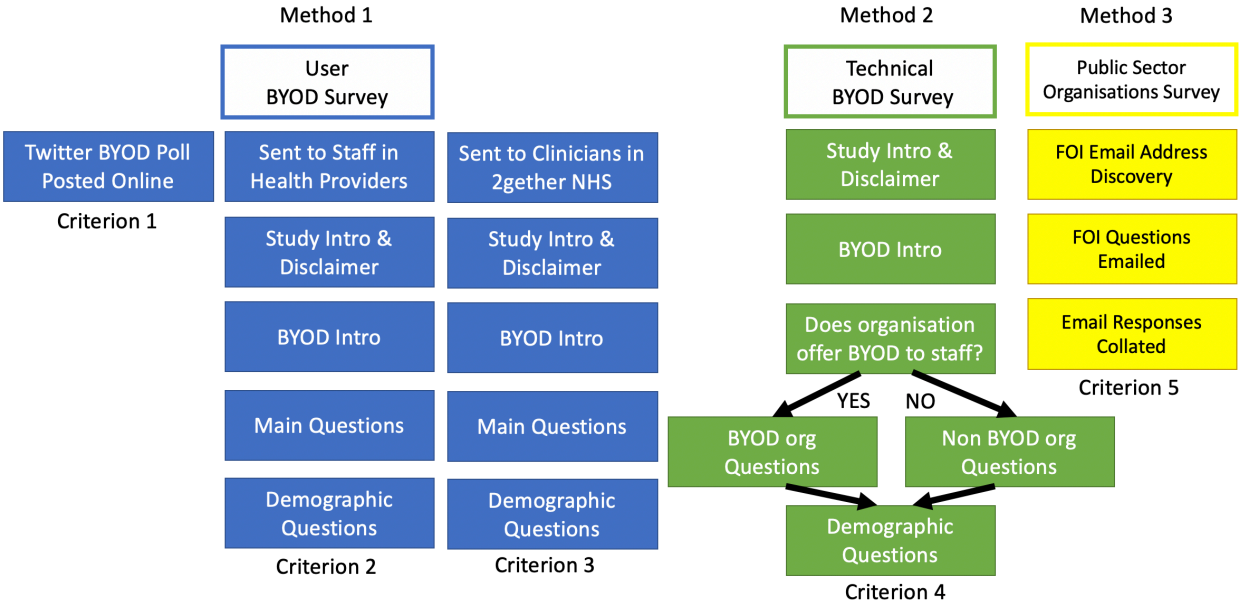


Figure 5. *Summary of survey pathways.*

Interview Sampling Criteria and Rationale

Criterion 1: Staff working for healthcare providers including NHS, social care and 3rd sector who responded to the user survey. Random selection ensuring respondents with a variety of views are included.

Format: Telephone and email interviews using questions provided in appendices.

Rationale: This sample will gather a base population against which 2gether's responses can be compared.

Outcomes: To obtain a more in-depth understanding of users' feelings towards BYOD. Responses will be analysed and compared against those gathered via Criterion 2.

Criterion 2: Clinicians working in the community for 2gether who responded to the user survey. Random selection ensuring respondents with a variety of views are included.

Format: In-person and telephone interviews using questions provided in appendices.

Rationale: This criterion will enable understanding of the perceived benefits of BYOD within the patient-facing workforce at 2gether.

Outcomes: To obtain a more in-depth understanding of user feelings and willingness to engage with BYOD. Responses will be analysed and compared against those gathered via Criterion 1.

Criterion 3: NHS technical staff currently supporting BYOD who responded to the technical survey. Random selection ensuring respondents with a variety of views are included.

Format: Telephone and email interviews using questions provided in appendices.

Rationale: This sample will gather understanding about implementation approaches with a BYOD enabled NHS organisation.

Outcomes: To obtain more understanding about the pros and cons of BYOD and the challenges involved with rollout, support, and maintenance. This will contribute evidence and best practice to support the development of an implementation strategy.

Criterion 4: NHS technical staff who don't operate BYOD who responded to the technical survey. Random selection ensuring respondents with a variety of views are included.

Format: Telephone and email interviews using questions provided in appendices.

Rationale: This sample will gather an understanding of views from a non-BYOD NHS organisation and provide insights into their perceptions and idealistic approaches to BYOD before they progress with it.

Outcomes: To obtain more understanding about the pros and cons of BYOD and the challenges involved with rollout, support and maintenance. This will contribute evidence and best practice planning concepts to support the development of an implementation strategy. It may also discover NHS organisations who have declined to implement BYOD and their reasoning for this.

Interview Sampling Recruitment Strategy and Rationale

The sampling strategy for interviews is maximum variation (Glasser and Strauss, 1967) because it allows the 'possibility of a greater range of application by readers and consumers of the research' (Merriam & Tisdell, 2016). Listening to a range of views from users and technologists will ground the research in reality, enabling more transferrable output from the study. Interview participants will be selected from survey respondents and will include different views and organisation types.

Given the limited time available the researcher decided to plan for 3 respondents for each interview criterion, giving a total of 12 interviews in total (Table 6).

Interview Criterion	Number of interviews planned
1: Staff working for healthcare providers including NHS, social care and 3rd sector	3 survey respondents from different organisations
2. Clinicians working in the community for 2gether	3 survey respondents
3. NHS technical staff currenting supporting BYOD	3 survey respondents from different NHS organisations
4. NHS technical staff who don't operate BYOD	3 survey respondents from different NHS organisations

Table 6. *Criterion summary for interviews.*

Survey and interview responses will be mapped to a value and graphed against other respondents (as shown in Figure 6) to illuminate trends and outliers enabling the discovery of a range of views and highlighting worthy interview candidates from surveys.

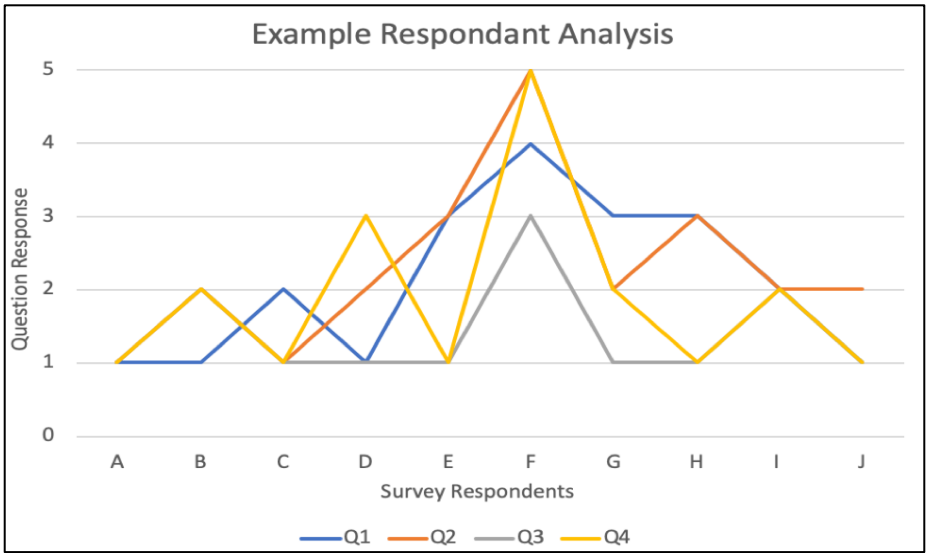


Figure 6. *Example graphed responses to aid discovery of variation.*

Consideration will be given to questions to ensure a variety of types are used (Patton, 2015), to stimulate a range of responses. An example interview guide showing question types for technical BYOD interviews is provided below in Table 7.

#	Question	Question Type (Patton, 2015)
1	How long has your organisation operated BYOD?	Knowledge
2	What was your approach to implementation? Any software products in use? Any limitations	Experience & Behaviour
3	What can and can't users do? What type of devices are supported? Do you offer BYOD to all staff?	Knowledge
4	What have been the biggest challenges?	Experience & Behaviour
5	What have been the benefits?	Opinion & values
6	Do you feel BYOD has been a success for your organisation?	Feeling, Opinion & values
7	What has the response been like from users?	Opinion & values
8	How well do users maintain their devices and keep the OS and Apps updated?	Knowledge
9	What is your approach to audit?	Experience & Behaviour
10	Have you had any data breaches or issues because of BYOD?	Experience & Behaviour
11	Do you feel access and equality is effectively managed in relation to BYOD?	Feeling, Opinion & values
12	What differences have your seen in approaches to work because of BYOD?	Experience & Behaviour
13	What impact on IT operating costs has BYOD caused?	Knowledge
14	If you needed to implement BYOD again in the future what would you do differently?	Hypothetical
15	Do you have a BYOD policy? Can I have a copy?	Knowledge

Table 7. *Interview guide for criterion 3. NHS technical staff currently supporting BYOD.*

Data Collection and Instrumentation

A range of methods have been chosen to collect data starting with the initial broad questions and becoming increasingly granular through research, surveys, targeted surveys, interviews investigating specific questions and document review. Figure 7 shows the questions considered by the researcher to aid investigation and discovery.

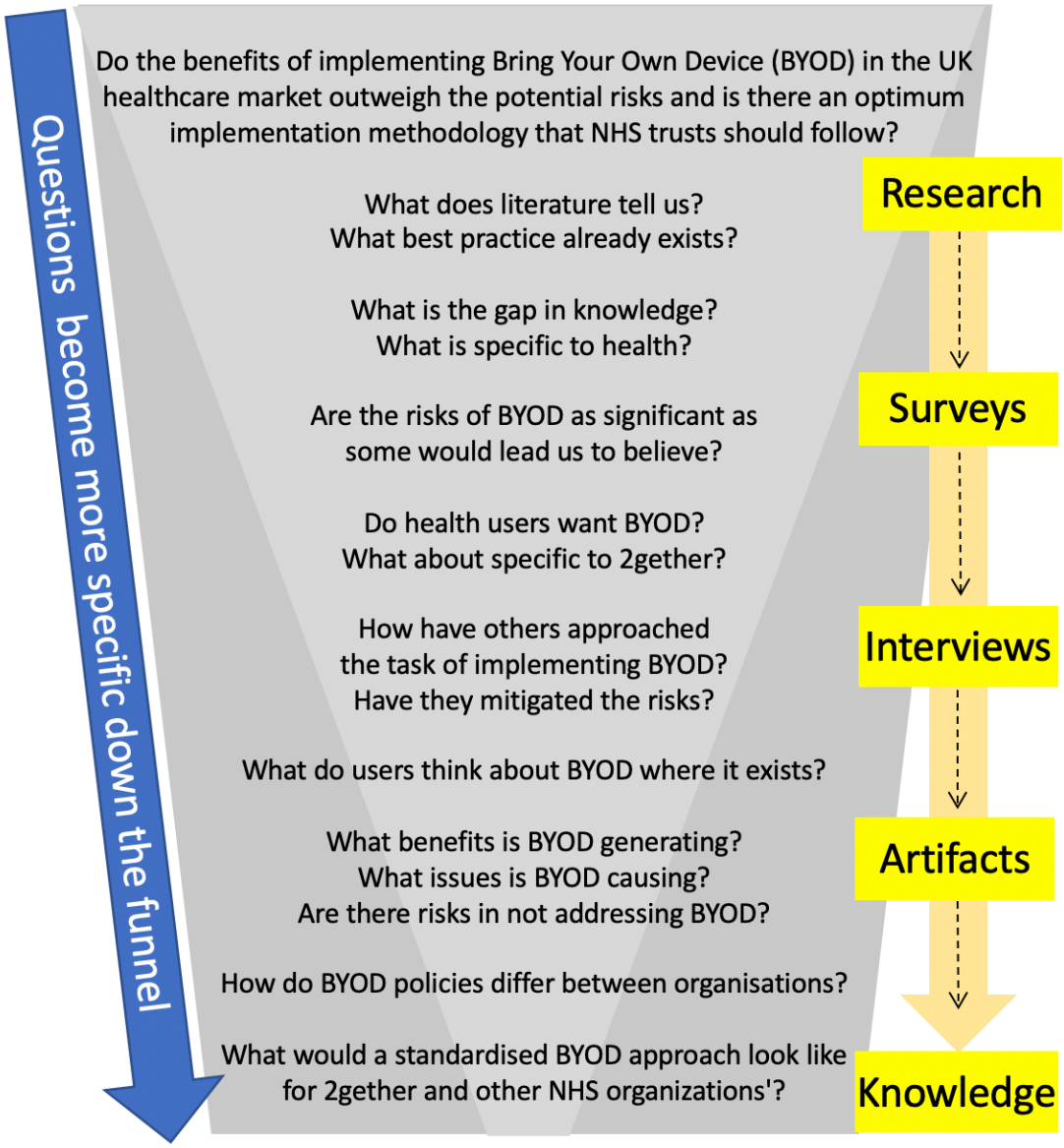


Figure 7. *Problem statement worksheet.*

Twitter will be used for a high-level single question initial survey with a link to the main user and technology surveys. SurveyMonkey.com was found to be a trusted resource which provided a clear and simple presentation of a range of question types including the ability to order a set of statements by priority.

A survey strategy was adopted which considered numerous factors to improve response rates (Oppenheim, 1992). For instance, the survey included an advance disclaimer to ensure the respondent understood there was no pressure on them to complete the survey. The email address of the researcher was provided at the start and end of the survey to provide a contact point for any questions or concerns respondents may have. A short explanation of BYOD and the research was provided to give context to the respondent. The survey was set up to be confidential with a limited number of questions to engage as many respondents as possible.

Factor	Survey Design Application
Explanation	Introduction about topic at start
Sponsorship	Explanation about MSc and why
Publicity	Via multiple routes
Incentives	Offered research output if interested
Confidentiality	Promised to keep involvement confidential
Reminders	Regular reminders to likely respondents
Appearance	Presented clearly via trusted survey platform.
Length	Minimal questions to maintain interest
Rapport	Experience used to demonstrate credibility Networks used to gather respondents

Table 8. *Factors used in survey design (Oppenheim, 1992)*

Interviews will be be conducted via telephone or email for each selected candidate. They will be scheduled as formal conversations with a structured list of open questions aimed at encouraging as much information gathering as possible. The questions will augment survey data with real-world experience and detail behind survey responses. Three sets of interview questions will be created, one for users and two for technical respondents to cover both BYOD and non-BYOD organisations. Interviews will be recorded and analysed.

The study will seek to collect a range of existing BYOD policies from NHS organisations to research areas of consistency which can contribute towards an updated national policy. The existing NHS Digital policy is generic and limited in scope (NHS Digital, 2017a). The study will request policies via NHS forums and networks in the hope to gather a good selection. Policies may also be obtained via website searches and FOI requests. The policies will provide a fixed point to inform the study on approaches, procedures and support offered by existing NHS BYOD schemes. A review of policies will be undertaken to compare approach and themes. The research will also consider expert best practice from the National Cyber Security Centre and The Information Commissioners Office (ICO).

Data Analysis

Data will be analysed using a scoring methodology which will graph data points and compare response groups providing an indicative temperature of the feeling towards BYOD in the NHS nationally and locally. Interviews will be recorded and notes taken. The notes and recordings will be analysed to look for common themes, important quotes or significant issues that require attention. Technical research will depend on good interview output to gather implementation experience and learning and therefore questions will be critical.

Credibility and Trustworthiness of Data

The online survey will only allow one response per device minimising the likelihood of multiple submissions from the same respondent. Insider/outsider status issues (Merriam & Tisdell, 2016) will be minimised because the researcher is well known both internally and externally from work on national projects. The researcher is experienced in both the technology under review and has high levels of rapport because of experience delivering services with users. The researchers learning experience via the NHS Digital Academy will help to ensure listening and understanding from the user's environment is prioritised and valued. Survey questions are all optional to avoid any individual respondent feeling pressured to answer a question that is not relevant or too sensitive to answer. This helps ensure responses are a true reflection of the user's feelings.

Validity and Reliability of Data

The study will use multiple sources of information and multiple methods to triangulate both local and national perspectives to shore up the internal validity of a study (Merriam & Tisdell, 2016). This approach will generate a wide dataset to triangulate and validate data. Surveying both users and technical specialists will provide validation and reliability to assure the study findings offer consistency.

It is likely to be more difficult to obtain responses from clinical staff who do not engage with technology and therefore additional effort will be made to engage this cohort by contacting department managers and clinical leads. The survey will collect information on respondent roles and therefore pulling out clinical responses will enable a separate analysis to give clinical percentages and feedback as much focus as non-clinical respondents.

There are multiple constructs of reality and individual experience for any given phenomenon (Merriam & Tisdell, 2016). Interviews will aim to recognise this in relation to past experience of NHS technology system implementation. There may be bias in user perspective related to the type of data they utilise and the differentiation in risk each individual perceives. Interviewees will be asked why they feel the way they do and what drives their responses to bring an understanding of their perspective and experience. Comments and issues shared by IT specialists via interviews will provide technical credibility when compared with one another and with external research documents.

Ethics and the Role of the Investigator

The researcher will include a disclaimer to make it clear the survey is part of a research study and not a part of regular employed work. It will also make clear the study is optional and all responses will be kept confidential (Figure 8). A contact email will be provided to allow respondents to ask questions. Interviews will be recorded (subject to consent) but never shared and will be deleted as soon as key data has been extracted. Those who choose to take part will be offered a copy of the final study output when completed.

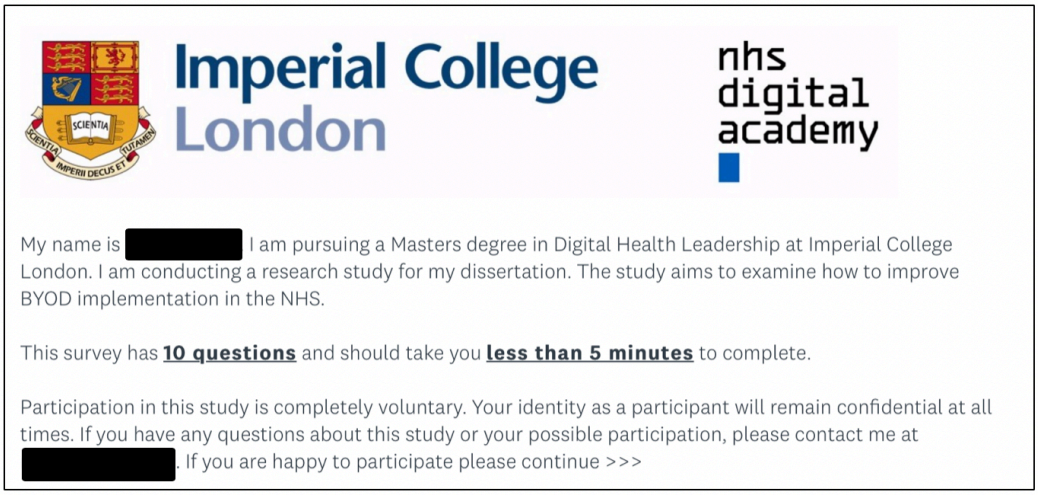


Figure 8. *Survey disclaimer.*

Questions will be posed with as minimal bias as possible but it needs to be recognised that the researcher has a known interest in BYOD which will likely generate some bias (Merriam & Tisdell, 2016). The targeting of both internal and external opinions via surveys and the interviewing of survey respondents at the extremities of responses will aim to minimise bias. Without researcher interest and inquisitiveness, the BYOD topic would not have been selected and the study hopes to add to the body of knowledge for the benefit of all.

Limitations and Delimitations

The study will investigate how clinicians feel about using BYOD in comparison to a wider field. The research aims to understand if clinicians believe the benefits outweigh the risks. The research will also investigate how NHS technical staff feel about BYOD and gather experiences of those who have implemented solutions to produce a new collection of best practice. The researcher won't directly discuss the impact of BYOD on NHS organisations or users.

The surveys used will be simple and ask high-level questions. Interviews will investigate deeper into experiences but won't address accessibility, digital literacy and equality, the detailed impact to work/life balance, or the environment. The study will review and analyse the data collected which will be assumed truthful. The instruments used aim to ensure data accuracy and authenticity to a reasonable degree. Survey distribution will predominantly be via Twitter, LinkedIn and email which will widen the respondent pool available although local NHS staff will be directly engaged.

BYOD is the topic of study and therefore Choose You Own Device (CYOD) is out of scope but certainly warrants further study, for instance, could CYOD and BYOD be delivered from the same infrastructure and revolutionise IT deployment and support models of the future?

CHAPTER FOUR: DISCUSSION

Introduction

The purpose of this chapter is to report the findings of the collected data. After collection the data were reviewed, analysed, and triangulated to understand and address the study's research question. The research question for this study is: Do the benefits of implementing Bring Your Own Device (BYOD) in the UK healthcare market outweigh the potential risks, and is there an optimum implementation methodology that NHS trusts should follow?

Data Collection Schedule

Online surveys took place from 27th August to 11th October 2019 using Survey Monkey. An online poll was run on Twitter from 28th August to 30th August 2019. Interviews were conducted via telephone and email from 20th September to 29th October 2019. FOI Requests were sent out on 24th November 2019 and responses received between 25th November and 5th January 2020. Policies were gathered via Surveys, Interviews and FOI Requests. Table 9 lists the data collection schedule.

Date	Location		Activity
27/08/2019	Online Survey		User Survey opened (SurveyMonkey.com) Technical Survey opened (SurveyMonkey.com)
28/08/2019	Online Survey	10pm	Poll opened (Twitter)
30/08/2019	Online Survey	10pm	Poll closed (Twitter)
20/09/2019	By Telephone	11:30	Interview (Criterion 1)
23/09/2019	By Telephone	12:00	Interview (Criterion 2)
25/09/2019	By Telephone	15:00	Interview (Criterion 2)
30/09/2019	By Telephone	10:00	Interview (Criterion 4)
11/10/2019	Online Survey		User Survey closed (SurveyMonkey.com) Technical Survey closed (SurveyMonkey.com)
21/102019	By Email	09:30	Interview (Criterion 1)
		09:45	Interview (Criterion 1)
		10:30	Interview (Criterion 1)
		12:00	Interview (Criterion 2)
		13:00	Interview (Criterion 3)
		14:30	Interview (Criterion 1)
		20:00	Interview (Criterion 1)
22/10/2019	By Email	15:30	Interview (Criterion 1)
23/10/2019	By Email	19:30	Interview (Criterion 3)
25/10/2019	By Email	15:30	Interview (Criterion 1)
29/10/2019	By Email	10:00	Interview (Criterion 4)
24/11/2019	By Email	13:30	FOI request sent out to 1,300 organisations
05/01/202	By Email	13:30	Collection of FOI requests closed.

Table 9. *Data collection schedule.*

Study Findings

The study investigated the benefits and risks of BYOD to understand whether it offered a viable approach for 2gether NHS Foundation Trust. Research was conducted via a number of surveys

and interviews which engaged users and organisations. Collection and review of policies provided intelligence on approaches taken in a range of organisations.

There is certainly appetite for BYOD, although enthusiasm varies by organisation, role and individual preference. Most organisations believe staff are already using their own devices at work regardless of policy. Efficiency benefits can be significant if the implementation engages users effectively, if risks are managed and if clear policies are developed. Clinical staff have significant concerns about data security and the pressures BYOD could place upon them; organisations such as 2gether should give this serious consideration.

Do users want BYOD?

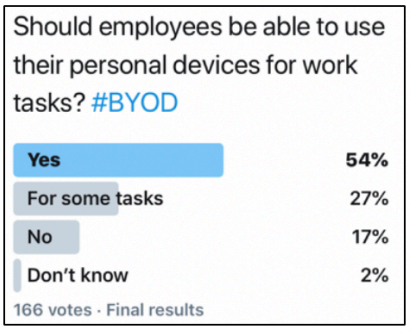


Figure 9. *Twitter poll result*

Generally, yes; but in the NHS it is not so simple. Users want the flexibility of BYOD although this desire to use personal devices at work does come with caveats because of the complex data and pressures that exist in the NHS. The Twitter poll (Figure 9) revealed 81% felt employees should be able to use personal devices for at least some work tasks. 70% of respondents to the healthcare user survey said their first reaction to BYOD was positive, although 2gether respondents (Figure 10) were less convinced being split 50/50, perhaps because a greater proportion of respondents were from clinical backgrounds (Table 10). Even so, 50% of staff using BYOD could still have a significant impact to organisational effectiveness and if BYOD were available many say they would sign up (Table 11).

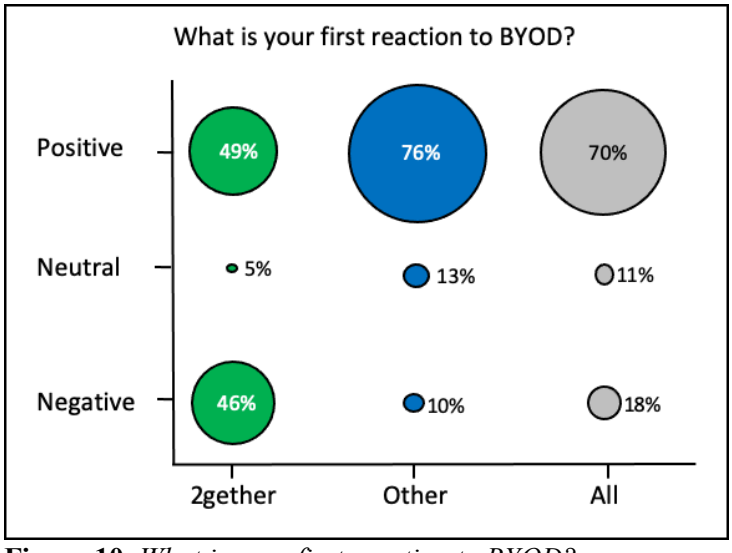


Figure 10. *What is your first reaction to BYOD?*

Respondent role type		
Group	2gether	Other
n=	41	144
Clinical	63%	41%
Non-Clinical	37%	59%

Table 10. *User survey respondent* type *(clinical or non-clinical).*

If Bring Your Own Device were available today, how likely would you be to sign up?							
Organisation Type	2gether	Other	All	+ve v -ve	2gether	Other	All
n=	41	144	185	n=	41	144	185
Extremely likely	34%	42%	41%	+ve	54%	80%	74%
Very likely	12%	24%	21%				
Somewhat likely	7%	14%	12%				
Not so likely	12%	13%	12%	-ve	46%	20%	26%
Not at all likely	34%	8%	14%				

Table 11. *Would you sign up to BYOD if it were available today?*

The clinical divide

Throughout interviews the biggest concern from clinicians was patient data security and work / life balance. These factors in most cases were sufficient to cause outright rejection of BYOD with quotes such as 'intrusion on to personal time, risk of IG too great', 'would probably lead to a divorce if I couldn't easily turn off work messages when I got home' or simply 'Not happening mate'. Senior consultants were concerned BYOD could make it too easy to get intrusive alerts or check up on critical patients and the duty of care would then extend 24x7 with no ability to switch off. There were a few individuals in senior clinical roles who were evangelists for BYOD, one (non 2gether) gave examples how using EHR systems on a personal smartphone was revolutionary. Another clinician explained that for 2gether's crisis team, smartphone access to real time patient information would avoid return visits to the office improving efficiency. There was a desire for more freedom in General Practice and disappointment that recent publications prohibit BYOD (NHS England, 2019b).

Other pro-BYOD interviewees were non-clinical office-based users and this group were overwhelmingly in favour of BYOD subject to appropriate controls. This group access clinical data less often and have roles where there is a need for innovative tools which can be more freely accessed via BYOD. The concern about patient data in reality demonstrates strong information governance skills across the NHS which should be recognised and applauded. In reviewing organisations who already offer BYOD there is a reflection of these concerns in the limitations as shown in Table 12 (see page 41) and similar reduced appeal for access to write patient data in both BYOD and non-BYOD organisations as per Table 13.

Benefits and Risks

100% of user survey respondents under 25 years old considered BYOD to be definitely or probably beneficial for the organisation regardless of role. In the technical survey this 100% approval

rate extended to age 35, supporting the expectation of younger generations for on-demand access to smartphones (Ofcom, 2018). It is likely that offering BYOD would make 2gether a more attractive employer to this cohort of individuals. Most respondents could see benefit from using BYOD and Figure 11 shows the impact of introducing BYOD in 2gether could be significant, increasing the use of Videocalls from 15% to 43% potentially transforming how communication takes place between the service user and caregiver. The ability to demonstrate apps with patients and service users was seen as positive and there was a significant desire for access to patient data on the move. Results were even more pronounced in the non-2gether respondents (Figure 12) especially where benefits were related to accessing clinical data.

The interview responses reinforced the theory users could be more productive and innovative on devices of their choice which they were used to working with and several were already actively using personal devices including laptops at work. Interviewee 12 explained how they setup multiple profiles to separate work and personal usage. Interviewees questioned organisational capacity to support BYOD onboarding and offboarding processes. Organisations who had implemented BYOD rated data security their highest risk and rated support impact the lowest (Table 14).

Interviewees responses were rated between 1 (anti-BYOD) and 5 (pro-BYOD) as shown in Figures 13 and 14. In most cases technical and non-clinical interviewees were more positive about the potential of BYOD (Table 15). Overall the responses were average or below. There are clear benefits from BYOD but the risks are viewed as too high at present in a clinical environment. As solutions develop it is likely some of the barriers to entry will reduce and BYOD will be seen as increasingly viable. BYOD is more likely to be beneficial today in non-clinical roles and this is where 2gether should focus initial BYOD implementation efforts. There is a need to find solutions to switch off alerts from BYOD systems when users are not at work. For clinical staff this is not the usual 9-5 and there is a big opportunity to develop more intelligent solutions which link clinician work patterns to BYOD alert settings.

Focus on cost and value

There was recognition that device savings could be beneficial for the organisation but concerns were raised about how staff could revert back to organisational devices if budgets had been reduced. Savings from reduced IT support are unlikely as a result of BYOD and therefore focus

should be on productivity benefits where the study found strong congruence. Interviewee 2 commented positively on the reduction in environmental cost of using a single device but ultimately believed the risk of work spilling into personal life was of paramount importance and warranted use of multiple devices.

Who should fund devices generated a significant disparity in responses. Most respondents believe the organisation should provide some level of financial compensation for using their own device (Table 16) but organisations who already offer BYOD unanimously demonstrated this is not common practice (Table 17). There is more to do to understand how staff using BYOD without remuneration feel and this model, whilst prevalent, reinforces the need to make BYOD optional. Concern about responsibility for replacing devices damaged in the line of duty was raised often and this is something 2gether would need to consider in its policy. Without support for accidental damage, take-up could be stifled but there is a need to ensure equity and prevent abuse.

Several interviewees commented on the issue of Digital Equity and this raises a number of questions. Could a BYOD model result in a two-tier organisation where those who can afford or choose to prioritise having new personal devices are able to work faster and use new tools? It is clear some individuals value access to a modern device above cost because of the benefits it offers. Could those who are unable or choose not to replace their device frequently be frozen out of new working paradigms? Will BYOD and device culture allow the younger generation to be more productive than their peers? How will organisations like 2gether address this issue and restore fairness to the workplace? Could a Choose Your Own Device (CYOD) approach be an option where employers offer more choice and bridge the clinical divide where there is a need for separation between work and personal systems? There are no doubt legal and discriminatory factors present that need careful consideration.

Data Analysis

On the following pages a number of tables and figures are presented which provide summaries of the research findings. These can be studied on their own, each is referenced from sections of this report.

Does your organisation limit what can be accessed via BYOD?	BYOD Org
n=	12
Does not allow write access to patient information	58%
Does not allow read access to patient information	33%
Does not allow access to users own personal files / data	33%
Does not allow access to text messaging or WhatsApp	25%
Does not allow user to download any apps user chooses for work tasks	17%
Does not allow access to work email	0%
Allows text messaging for work via a custom application	17%
Allows access to curated list of approved apps for work tasks	8%

Table 12. *Limits BYOD organisations place on systems.*

What work tasks do you (or would you) allow staff to complete on their personal devices?	BYOD Org	Non-BYOD
n=	14	26
Voice communication	86%	85%
Text messaging services	79%	81%
Video calls (e.g. Facetime or Skype)	57%	77%
Work email and calendar	100%	85%
Edit work documents	57%	58%
Ability to demo self-help apps to service users	50%	54%
General apps for health practitioners	64%	54%
Apps that provide read access to patient records	43%	42%
Apps that allow write access to update patient records	43%	27%
My organisation would never allow use of BYOD for anything	0%	8%

Table 13. *Tasks BYOD organisations allow on personal devices & what non-BYOD would allow if they offered BYOD.*

How would you rank the following risks in relation to BYOD?		
Group	BYOD Org	Non-BYOD
Data loss from staff members personal device	1st	5th
Increase in unpatched devices	2nd	2nd
Network capacity issues	3rd	6th
Rise in staff non-compliance with policies	4th	3th
Reputational damage caused by BYOD issues	5th	4th
Increased user support requirement	6th	1st

Table 14. *Difference between BYOD and non-BYOD organisational technical risk rating.*

Interview Criterion		Average	n=
1	NHS	2.6	9
	NHS clinicial	2.2	7
	NHS non-clinical	3.9	2
2	2gether clinician	2.4	3
3	Technical BYOD	3.9	2
4	Technical non-BYOD	3.3	2

Table 15. *Interview average rating per criterion.*

Users: Should the organisation contribute towards your BYOD costs?			
Group	2gether	Other	All
n=	41	144	185
Yes	83%	60%	65%
No	5%	27%	22%
Don't Know	12%	13%	12%

Table 16. *Should the organisation fund BYOD?*

Tech Staff in BYOD orgs: Does your organisation contribute towards staff costs of using their own device at work?	BYOD Orgs
Yes	0.00%
No	100.00%

Table 17. *Do existing BYOD organisations fund BYOD?*

Do you think staff already use personal devices for work tasks?	
Group	Non-BYOD
n=	26
Very likely	65%
Likely	27%
Neither likely nor unlikely	8%
Unlikely	0%
Very unlikely	0%

Table 18. *Do staff already use BYOD?*

Does your organisation have any of the following?		
Group	BYOD Org	Non-BYOD
n=	14	26
BYOD Policy	71%	0%
Acceptable Use Policy	71%	73%
Social Media Policy	78%	65%
Security Policy	85%	92%
None of the above	0%	4%

Table 19. *Policies in organisations responding to the technical survey.*

Do you have a BYOD audit process to ensure policy is adhered to?	
Group	BYOD Orgs
n=	14
Yes	36%
No	64%

Table 20. *BYOD organisations position on audit processes.*

How many staff in your organisation currently use BYOD?	BYOD Org
n=	14
don't know	3
up to 500	5
500 - 1000	4
above 1000	2

Table 21. *How many staff use BYOD solutions in the organisations who offer it.*

Is BYOD something you see as beneficial for the organisation?		
Group	BYOD Org	Non-BYOD
n=	14	26
Definitely beneficial	50%	42%
Probably beneficial	43%	39%
Unsure if beneficial	0%	15%
Probably not beneficial	7%	4%
Definitely not beneficial	0%	0%

Table 22. *Is BYOD beneficial for the organisation? BYOD and non-BYOD views compared.*

Is your organisation considering BYOD?	
Group	Non-BYOD
n=	26
Definitely	8%
Probably	27%
Not sure	53%
Probably not	8%
Definitely not	4%

Table 23. *Non-BYOD organisations considering BYOD.*

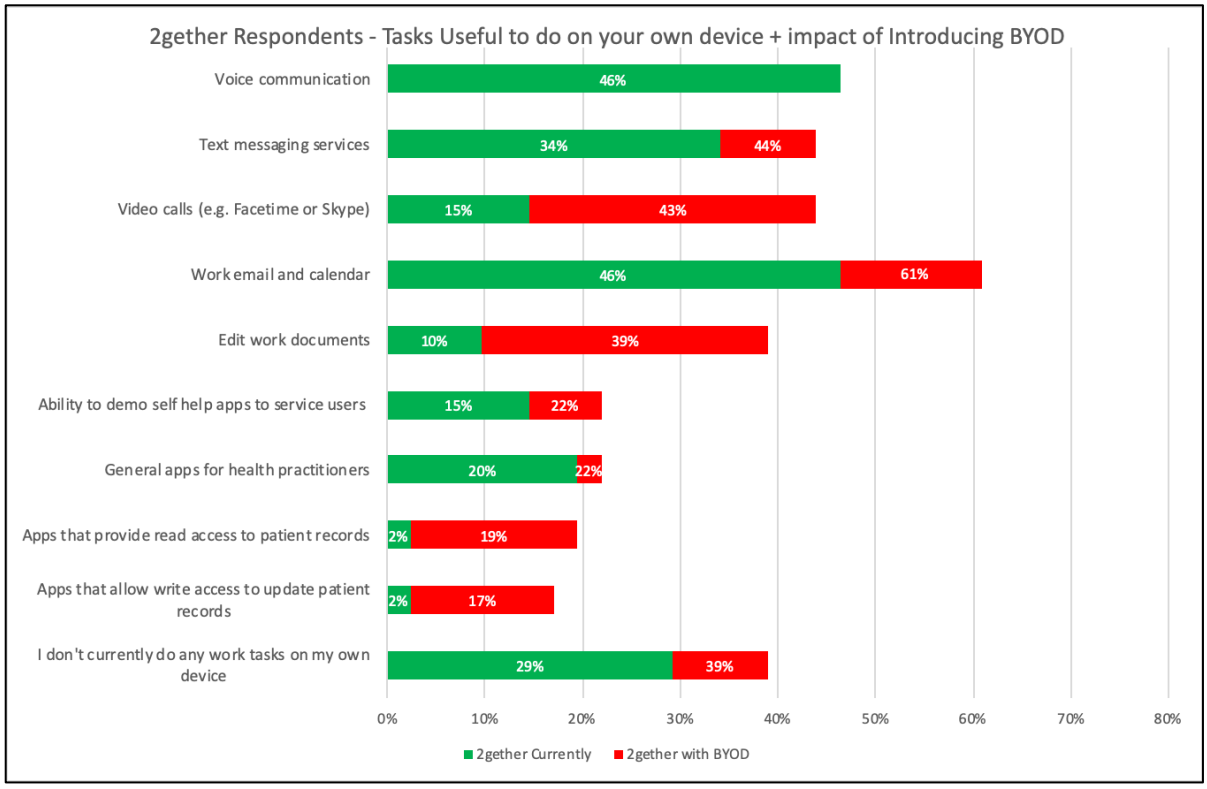


Figure 11. *2gether user survey respondents showing in red how BYOD could change ways of working.*

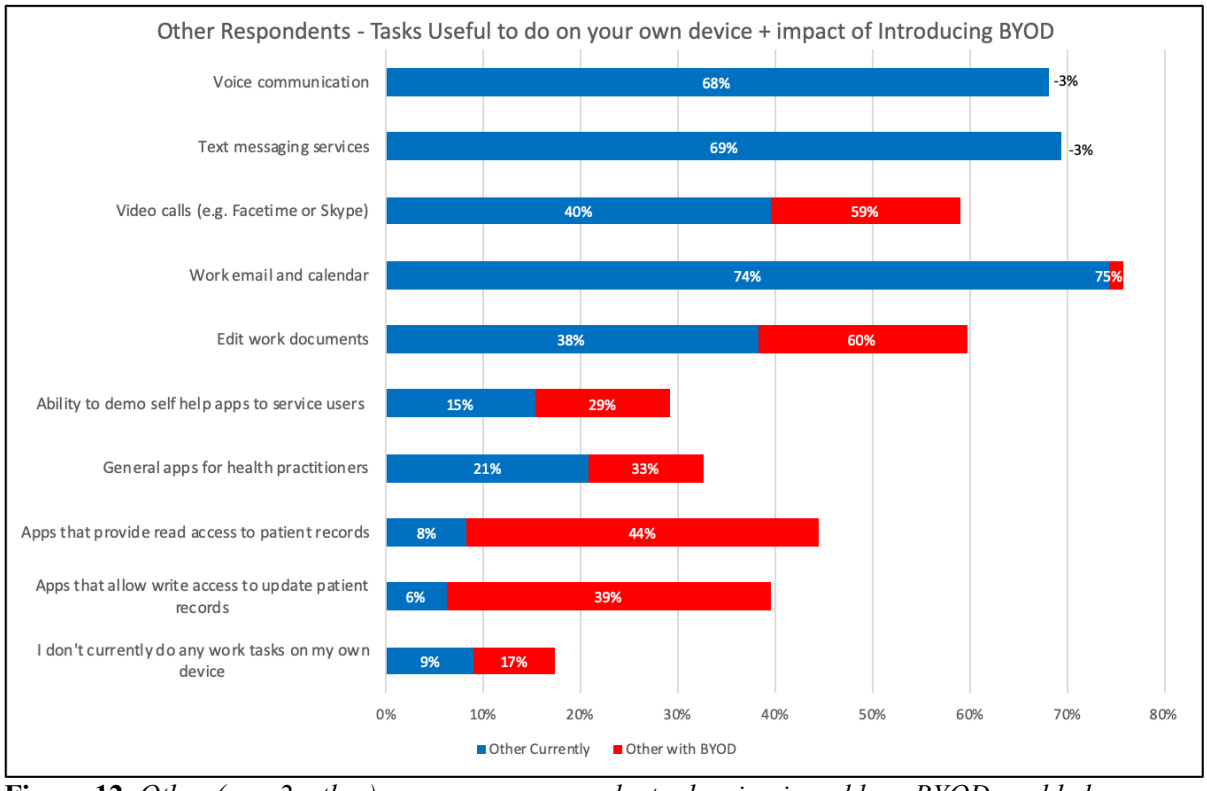


Figure 12. *Other (non-2gether) user survey respondents showing in red how BYOD could change ways of working.*

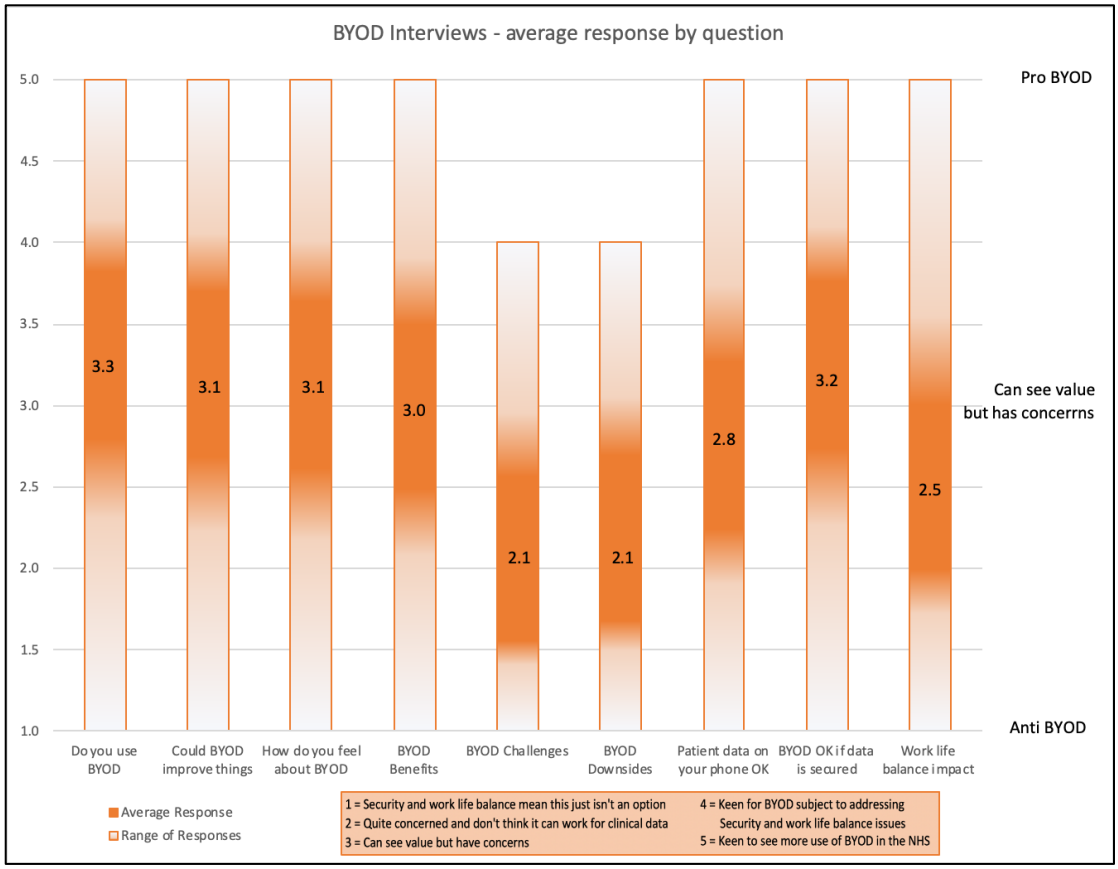


Figure 13. *Interview response range by question showing average rating in solid region.*

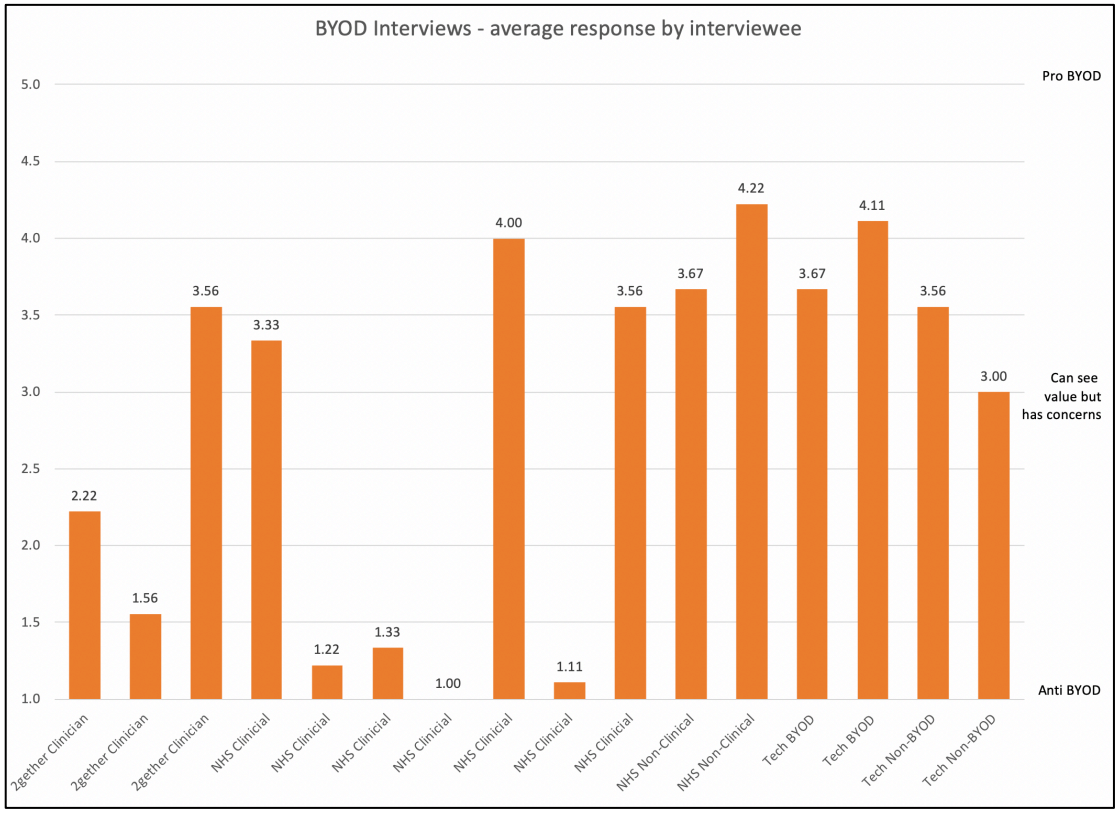


Figure 14. *Individual interviewee total rating across all questions. Interviewees shown by primary discipline.*

Policy Findings

92% of organisations not using BYOD thought it is likely or very likely their staff are already using personal devices for work tasks (Table 18). Organisations who actively dismiss BYOD leave themselves open to risk from users who will use it anyway. The policy review revealed good practice, especially by organisations with a dedicated BYOD policy, but many organisations said their BYOD statement was embedded inside IT security policies which made finding and understanding BYOD information difficult. 71% of BYOD organisations responding to the technical survey had a policy (Table 19) yet only 36% had an audit process (Table 20) to ensure users adhered to the stated policy. Without clear policies, such as the audit function, the risk to organisation data increases. Organisations that don't offer BYOD also don't have a BYOD policy (Table 19) and whilst this might sound a natural correlation it would actually be better to have a BYOD policy making it clear it was not supported. Without such clarity it is likely BYOD usage will grow organically without control. The survey revealed that organisations exist without clear understanding of the number of users they have using BYOD (Table 21).

Using the Freedom of Information act a wide range of government bodies were asked about their approach to BYOD and whether they had policies in place. The feedback placed the NHS as the second highest user of BYOD (Figure 15), although half of NHS BYOD trusts did not have a policy (Figure 16) which is a wider gap than other sectors.

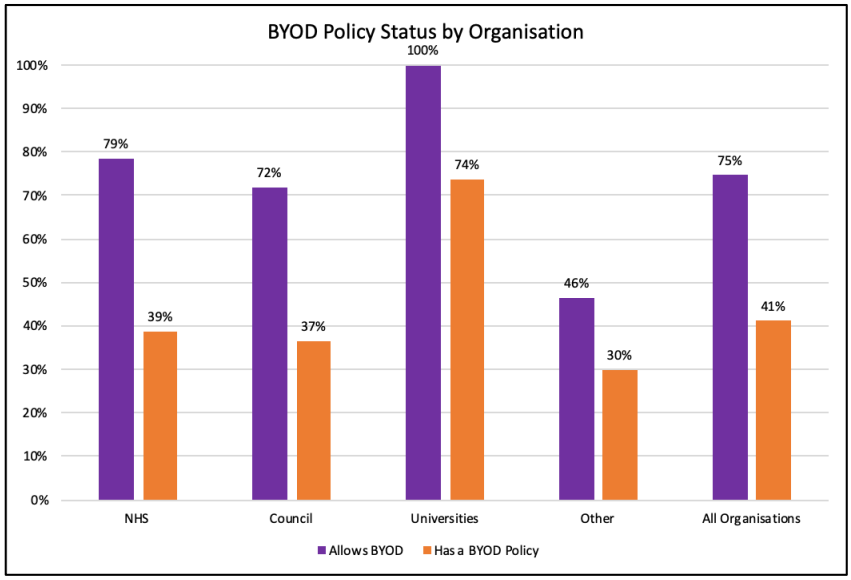


Figure 15. *Percentage of organisation groups responding to FOI who offer BYOD versus those with a policy.*

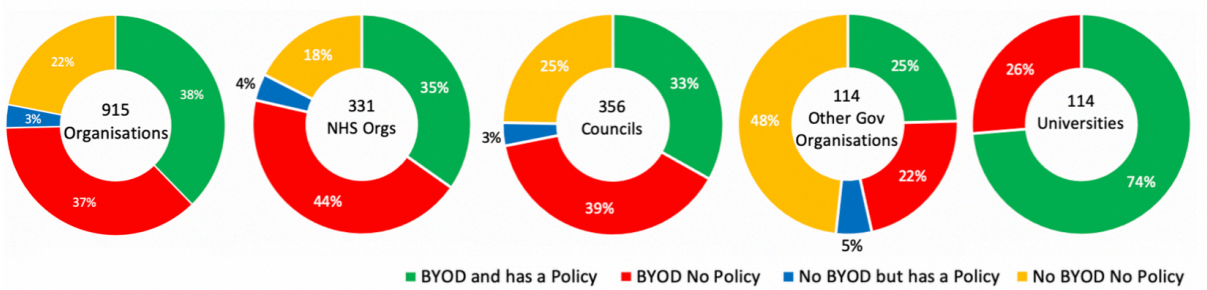


Figure 16. *BYOD usage and policies in the NHS and other sectors.*

The technological pace of change which makes BYOD attractive, has a consequence of making policies expire quickly. The majority of NHS polices are prescriptive and lack any flexibility to cover changing needs and are not updated frequently enough. Policies which are less prescriptive and more contract-based may reduce overall policy maintenance (Hallet and Aspinal, 2017). A wide range of polices were reviewed and some interesting excerpts are shown below (Table 24, Page 46). There were several policies that used ambiguous statements and others where the organisation's BYOD position was buried in 50 plus pages of complex technical standards. Most NHS BYOD policies were embedded within other policies (such as IT security, acceptable use and mobile working policies) with limited references to use of personal devices. The existing NHS Digital example BYOD policy template (NHS Digital, 2017a) is nearly 3 years out of date and is targeted at a very technical audience, this really needs to be updated and modernised.

One specific organisation policy worthy of review is that of NHS England (NHSE). Based on the FOI response NHSE allows BYOD only for NHSmail. NHSE does not have a BYOD policy, but stated it was covered by their Acceptable Use Policy (AUP). The relevant excerpt is provided below in Figure 17.

'At present personal devices are not supported by NHS England and NHS Improvement and support cannot be requested from corporate resources. It not advised or acceptable to process person identifiable data on a device which is not provided by NHS England and NHS Improvement. We remind staff that it is the responsibility of the user for non-NHS equipment being used, including maintenance and all reasonable security precautions.'

Figure 17. *NHS England Acceptable Use Policy excerpt* (NHS England, 2019c).

For NHS England staff, finding a statement on BYOD might be challenging as they would need to look for something referenced as the AUP. Once found, it would not be immediately clear this statement related to BYOD. Further, the whole statement is ambiguous. For instance, NHSE use NHSmail that supports Patient Identifiable Data (PID) but, policy states that it is not acceptable to

process PID on personal devices. The policy contradicts itself because users cannot control what they receive over a PID secure email system. The policy provides advice, but is advice mandatory? What are ‘reasonable security precautions’? All of this is confusing for users.

The NHS England ‘BYOD policy’ also represents NHS Improvement’s position. This causes yet more confusion because the CQC (who are part of NHS Improvement) do indeed support BYOD in their organisation for email, calendar and additionally the suite of Office 365 software.

Organisations with good policies

The better policies came from Universities and the best of all came from Councils many of whom had dedicated policies which provide clarity for staff. Good examples include, Essex County Council’s BYOD User Responsibility Policy which covered rules to keep data safe and how to report breaches or lost devices. Also included was information about costs, the fact they do not reimburse staff, and helpful links to other policies and documents such as ‘What can ECC see on my person device’ and ‘Responsibilities – Line Managers’.

The most comprehensive document was the Flintshire County Council BYOD policy which was fully dedicated to personal devices. It was clearly dated 2019-2022 on the front which not only indicated it was valid but also when it expired. Sections were clearly laid out and used language appropriate for a range of audiences. Scope of what could be used and the voluntary nature of the scheme was made clear. The purpose of the policy, how to keep data secure and how access support was also communicated. A policy similar to this could be useful as best practice for 2gether. Table 24 shows example statements from the policy document review. Some are unhelpful, ambiguous or age easily, others are very sensible.

Type	Policy Excerpt	Comment
Prescriptive	'The use of the camera on a mobile device to capture patient images is generally prohibited and may be only be used in exceptional circumstances with the image transferred securely for inclusion in patient records as soon as possible and then deleted from the device. The use of any camera must be undertaken in accordance with the Trust Medical Photography Policy.' (Aintree University Hospital NHS FT 2019: p.6)	Prescriptive and supports automatic compliance with Medical Photography Policy.
	'Staff should not use any unauthorised portable device or digital storage device for Trust business.' (Airedale NHS FT 2015: p.2)	Prescriptive Prohibition. A list of devices that are authorised would help.
	'Jailbroken Apple devices are strictly forbidden from accessing healthcare infrastructure.' (Berkshire Healthcare NHS FT 2019: p.2)	Prescriptive Prohibition and sensible but nothing about non-Apple devices.
	'Devices must be set to automatically lock after five minutes of inactivity.' (Cambridge University Hospitals NHS FT 2017: p.28)	Prescriptive and sensible. Unlikely to need to be changed.
	'The organisation is not responsible for the liability or reimbursement to staff for: - a percentage of the cost of their BYOD device, - data charges on their BYOD devices, - any damages or compensation in the unlikely event that personal data on their BYOD device is affected or lost.' (Cardiff and Vale University Health Board 2018: p.4)	Prescriptive and provides clarity. Interesting that the organisation doesn't want cost or any responsibility for user personal impact. Feels too one-sided.
	'Current devices approved for Bring Your Own Device use are listed below along with the minimum system requirements: - Android 4.4.2 or higher Smart Phones and Tablets - iOS 9 or higher iPhones and iPads' (Bath & Northeast Somerset Council 2019: p.2)	Prescriptive and will need to be regularly maintained. Trusts wouldn't want to support Android 4.4.2 (2013) or iOS 9.0 (2016) anymore and there have been many major releases since. It doesn't encourage users to maintain their devices with current software.
	'Devices that are shared - such as with other family members - cannot be used as a BYOD as there is an increased risk of information accidently being accessed by unauthorised users.' (Canterbury City Council 2018: p.3)	Prescriptive and sensible. Unlikely to need to be changed.
Contract based	'The key principle of personal device usage is that the user owns, maintains and supports the device.' (Ashford and St Peter's Hospitals NHS FT 2019: p.1)	Contract-based, not specific on devices or software supported just requires user to own, maintain and support themselves.
	'To eliminate the inconvenience of carrying and operating two phones – a work phone and a personal phone.' (Calderdale City Council 2019: p.2)	Contract-based, goal is to make life better.
	'The CCG is required to develop a BYOD Policy to reflect the increased mobility of the modern workforce. This in turn ensures that there is a resulting increase in user satisfaction/productivity and may also help to reduce capital expenditure on ICT assets (end user devices).' (Great Yarmouth And Waveney CCG 2017: p.5)	Contract-based, end goal to improve satisfaction and productivity whilst acknowledging possible savings.
Ambiguous	'It is not permissible to use personal IT equipment for Trust business purposes. The only exception to this is through a Trust approved BYOD (Bring You Own Device) service. *No such service exists at the time of the creation of this Policy.*' (Somerset Partnership NHS FT 2015: p.22)	Prescriptive, confusing and policy was over 5 years old.
	'Only Trust owned and managed devices should be used to connect to the Trust corporate network (via network port or Wi-Fi), in no circumstances should privately owned devices be used to connect to the corporate network.' (Royal Marsden NHS FT 2019: p.8)	BYOD is not referenced in policy and this statement does not prohibit it, just not on the Trust network.

Table 24. *Example BYOD policy statements.*

Implementation

93% of organisations using BYOD said it is definitely or probably beneficial, in non-BYOD organisations the figure remained high at 81% (Table 22). It was surprising that only 8% of these are definitely considering a BYOD project (Table 23) which feels worryingly low, given the acceptance it's happening anyway (Table 18). In technical surveys organisations implementing BYOD with similar software solutions had different views on the impact of support. One organisation said BYOD for 500 users caused an unacceptable workload, whereas a larger organisation using the same solution for 6000 users thought the overhead was acceptable. This suggests factors such as size, resource, ambition and culture are likely to impact implementation and discovering the optimum implementation method for your organisation is critical. Most existing BYOD organisations implemented systems with their own teams, many non-BYOD organisations say they would seek external support, perhaps because of internal knowledge gaps (Table 25).

What approach to BYOD implementation did your (or would your) organisation take?		
Group	BYOD Org	Non-BYOD
n=	14	26
Implemented internally with own team	79%	38%
Assisted by a supplier BYOD solution	7%	23%
Brought in professional expertise	0%	27%
Outsourced the solution	0%	8%
Other (please specify)	14%	4%

Table 25. *Implementation approach of BYOD organisations or that which a non-BYOD would prefer.*

Should 2gether decide to implement BYOD the organisation would benefit from a discussion with other NHS trusts with experience in BYOD, especially given the variability between BYOD and non-BYOD responses in the survey. Balancing the needs of general BYOD from specific clinical BYOD will need to be addressed within 2gether using appropriate engagement methods and will require the full support of the board.

Recommendations and Guidance for Action

Staff at 2gether are likely to already be using their own devices for work tasks (Table 18). Therefore, 2gether should at a minimum, produce a BYOD policy stating what is and what is not permitted. Given the potential benefits of BYOD it is recommended that 2gether review the BYOD Implementation Cycle (Figure 18) developed by the researcher during this study, which combines elements of Verbonav's five

steps and The Digital Transformation Compass (Westerman, Bonnet and McAfee, 2014) to increase governance focus, to reflect the needs of NHS data and to protect the people who deliver exemplary care.

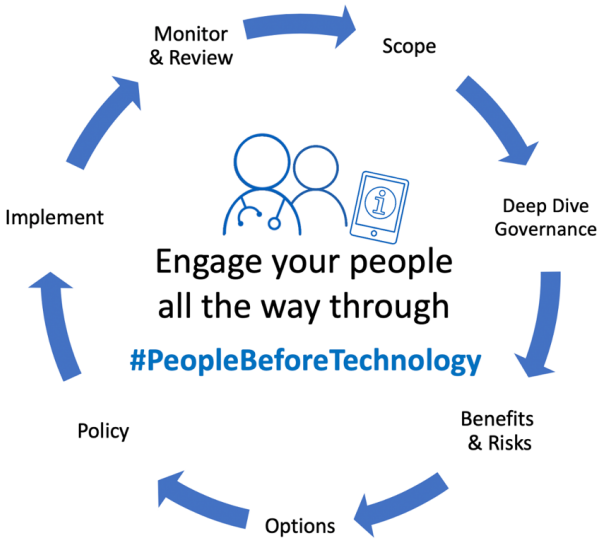


Figure 18. The BYOD Implementation Cycle.

Summary implementation advice based on this papers research is as follows:

1. Engage colleagues all the way through

Work closely with staff to review how BYOD can be beneficial for colleagues, the organisation and service users. Consult staff about ways they already benefit from using their own device. Have impartial experts available to provide guidance and advice to support the conversation. Use workshops to gather views and be willing to accept there will be differences of opinion. Listen to staff perspectives on the safety of patient data and the concerns about the potential impact to work/life balance. Clinicians need assurance the organisation won't proceed to offer clinical system access via BYOD on day one, their input and confidence needs to be highly valued. Gather a list of the areas where there is agreement BYOD could add value. Dig deeper into the areas of consensus and discuss the impact and risks openly and honestly. Form a group to take the project forward and include clinicians, IG leads, those with the biggest concerns, board members and those keen early adopters.

2. Develop scope

Agree on the initial objectives and outcomes. What are the specific use cases? Initially perhaps these will be business applications with wide appeal rather than clinical. Also consider applications which will make a difference to clinicians; perhaps rotas, secure messaging apps or reference data to support clinical practice. Talk with other similar organisations who already use BYOD about where they have

seen the maximum benefit. Once decided think about total number of users that could utilise the solution and who might form a subset to take part in a pilot to test solutions and assumptions.

3. Prioritise data governance

Review the planned scope and break down in detail what data will be required, where it exists and how it will be managed. Limit data to what is required to enable the anticipated outcome. Classify the types of information and have clarity on whether any is confidential or personal identifiable data (PID) and who currently owns it. Think about how data will be transferred, accessed and stored on devices. Prioritise presenting/streaming data to BYOD rather than storing data on devices. Be clear on data ownership recognising this responsibility applies regardless of processing device. Consider requirements for the NHS IG Toolkit from the start to ensure processes fulfil these. Review ICO best practice for BYOD implementations (The Information Commissioners Office, 2019).

4. Analyse benefits and risks

Baseline the current process and future benefits of the BYOD approach. Are there time, quality and cost benefits involved? BYOD has been linked to productivity gains, employee satisfaction, morale improvements, increased innovation and flexibility, employee retention and more. Think about how 2gether can measure these now and in the future. What are the risks involved in the proposed application of BYOD? Consider security risks, adoption barriers – perhaps caused by boundary theory, knowledge and training challenges, costs to implement and those of ongoing administration and management. Review options to mitigate and manage the risks documented.

5. Investigate technical options

Work with local organisations and those in a similar sector to 2gether who have already successfully implemented BYOD. Understand their challenges and the lessons learned. Many existing NHS BYOD organisations implemented with their own staff which brings local knowledge of the Trusts existing systems, policies and culture. This will be useful in 2gether but external support will bring in new ideas and help the project avoid blind spots caused by policy legacy or a lack of experience. Large scale rollouts have succeeded in having a low support impact and focusing on this will make the solution sustainable and cost effective. Look for technical systems which will provide the required controls. Most Mobile Device Management (MDM) solutions can be configured to protect data and devices without impacting personal user data. Investigate the market and test assumptions. Visit organisations using

different products to understand how they work in context. If you can, aim to isolate or containerise the 2gether BYOD apps and use a curated app store for staff, ensuring a process exists to amend the app list.

6. Build policy and processes

Develop a new stand-alone BYOD policy so staff know where to find the latest guidance. The recommendation is that organisations not make BYOD mandatory but rather that they offer it as widely as possible. Ensure expectations are clear from the outset using a mixture of prescriptive and contract-based statements. Assure staff about how BYOD systems are secured and what data might be accessible to the employer. Ensure the policy covers audit processes to monitor and review BYOD compliance. Address the issues of remuneration and digital equity and consider multi-level polices. Build a culture of trust and encourage staff to self-report issues to enable rapid resolution. Review NCSC's BYOD guidance (National Cyber Support Centre, 2016).

7. Implement

Develop an implementation plan. Rollout the chosen solution carefully and ensure comprehensive testing throughout. Provide training to colleagues as the solution is launched ensuring expectations are explicitly discussed such as the user need to maintain the device's software and to report any problems. Roll out to support staff first so that they can familiarise themselves with how the solution works. Work closely with colleagues to resolve issues as they occur.

8. Monitor and review

Monitor for compliance regularly throughout rollout. Review benchmarks pre and post implementation and follow up on audit outcomes. Conduct a systematic review of the project – use interviews and surveys to gain insight into how productivity and/or staff morale were impacted. Identify the actual benefits and costs. What issues were uncovered and how were they addressed? What was the support impact? Report progress and decide to scale up if all goes to plan. Think about another application or use-case.

Chapter Five: Conclusions

Linking Study Findings to National Priorities and Goals Around Digital Readiness and Digital Maturity across the NHS

NHSmail revolutionised the NHS by providing email and calendar access from personal devices and it has been widely adopted, advancing the NHS significantly. Many organisations have not progressed BYOD beyond email, perhaps because of technological and governance challenges. The rise of advanced consumer technology with its rapid refresh rates provides staff with more capable digital devices than available in the workplace. There is wide acceptance BYOD brings benefits and there is acknowledgement that staff already use personal devices at work, yet a lack of specific policies and implementation guidelines leave organisations at risk. Locally the NHS should prioritise BYOD policy development to ensure staff have visibility of what their organisation supports and restricts. Nationally the NHS should encourage trusts to produce simple, clear, accessible BYOD policies for their staff and perhaps CQC audits should stretch into digital practice to review the impact and clinical effectiveness of such technology.

Future Research Directions

This study has investigated current trends and feelings towards BYOD particularly within the NHS. It would be useful for this work to be extended to review existing NHS implementations and specific BYOD technologies which could form a suite of blueprinted solutions that could be tailored to any organisation. Digital equity was not investigated in this study and given the inclusive approach embraced within the NHS community this needs more thought to ensure technology division does not impact individual or operational service delivery, this issue extends into the remuneration models on offer.

There was limited engagement from third party healthcare partner organisations within the surveys conducted and further research into opportunities BYOD could offer to integrate data and systems for the benefit of the regional Integrated Care System (ICS) would be valuable. Policies reveal excellent practice in councils across the country and a review of BYOD which is more embedded in this arena may yield additional key findings and transferrable knowledge to aid the NHS development of practice standards.

The exponential increase in health-related Internet of Things (IoT) devices offers another avenue for research. Aggregating this personally collected data (by sensors 24x7) with core health record data could bring new insights and treatment opportunities. A new form of BYOD is beginning to emerge called Bring Your Own Data which allows individuals and organisations to contribute their own information into larger datasets offering the exciting promise of richer and more representative knowledge and information.

Conclusion

There is no single optimum implementation method for BYOD in the NHS but, this study has revealed there are nuances that are different in healthcare. Engagement is critical especially with clinical teams to ensure BYOD releases pressure rather than adds to it. BYOD adoption in the NHS can bring benefits if the risks are clearly articulated and addressed, and the boundaries of use are defined.

Every NHS organisation should have a specific BYOD policy regardless of whether the organisation supports BYOD. Providing a clear position on BYOD is essential due to the rise in default digital behaviours and assumptions that exist in the workforce. NHS organisations demonstrating significant benefits from BYOD should be given a platform to share their implementation achievements especially those who have resolved how to engage staff, securely manage clinical data and found solutions to digitally separate personal and work lives.

BYOD is embedded in organisations across the globe advancing efficiency, creativity and staff morale. Now is time for the NHS to adopt and bring to life the opportunities offered by this organic movement to modernise working practices, ensuring the NHS is ready for its future workforce.

Word count = 10,951 with headings and references, 10,270 without.

References

2gether NHS Foundation Trust. 2019a. *Website homepage.* Available from: https://www.2gether.nhs.uk/ [Accessed 10th May 2019].

2gether NHS Foundation Trust. 2019b. *About Us.* Available from: https://www.2gether.nhs.uk/about-us/ [Accessed 10th May 2019].

Ackerman, E., 2018. *Calculating The True Cost Of BYOD.* Available from: https://www.forbes.com/sites/eliseackerman/2013/05/28/calculating-the-true-cost-of-byod [Accessed 28th September 2019].

Aintree University Hospital NHS FT. 2019. *Mobile Device Management Policy.* Version 3.0. Page 6, Section 4.1.7. Policy obtained via FOI request 6639.

Airedale NHS FT. 2015. *Portable Computer Devices and Removable Media*. Version 2.0. Page 2. Policy obtained via FOI request ANHST REF 4599.

Ashford and St Peter's Hospitals NHS FT. 2019. *BYOD Information Security Policy Extract.* Page 1. Section 4.1.1.1. Policy obtained via FOI request FOI 7110.

Bath & Northeast Somerset Council. 2019. *BYOD Policy*. Page 2. Section 4. Policy obtained via FOI request 1794/19.

Berkshire Healthcare NHS FT. 2019. *Information Security Policy Extract*. Page 2. Policy obtained via FOI request 313.

Bresnick. 2013. *Despite security risks, BYOD helps nurses be more productive.* Available from: https://healthitsecurity.com/news/despite-security-risks-byod-helps-nurses-be-more-productive [Accessed 17th May 2019].

Calderdale City Council. 2019. *Privately Owned Mobile Device (BYOD) Policy and Disclaimer.* Version 1.7. Page 2. Section 2.2. Policy obtained via FOI request 1920168.

Cambridge University Hospitals NHS FT. 2017. *Information governance and information Security Policy*. Version 13. Page 28. Section 24. Policy obtained via FOI request 799.19.

Canterbury City Council. 2018. *Bring Your Own Smart Device Policy.* Version 4.0. Page 3. Policy obtained via FOI request 8268.

Capgemini Consulting. 2013. *Bring Your Own Device. It's all about Employee Satisfaction and Productivity, not Costs!* Available from: https://www.capgemini.com/resources/bring-your-own-device-its-all-about-employee-satisfaction-and-productivity-not-costs/ [Accessed 31st July 2019].

Cardiff and Vale University Health Board. 2018. *Bring Your Own Device-Local Procedure*. Version 1.1. Page 4. Section 2. Policy obtained via FOI request 19.471.

Care Quality Commission. (2019). *Overview and CQC inspection ratings for 2gether NHS Foundation Trust.* Available from: https://www.cqc.org.uk/provider/RTQ [Accessed 10th May 2019].

Chen, N. 2013. *How Much Can You Save?: A BYOD Cost Analysis*. Available from: https://www.repsly.com/blog/field-team-management/save-money-byod-cost-analysis [Accessed 31st July 2019].

Cidon, A. 2015. *The only way to control BYOD is to embrace it.* Available from: https://www.hcinnovationgroup.com/cybersecurity/bring-your-own-device-byod/article/13007153/the-only-way-to-control-byod-is-to-embrace-it [Accessed 30th July 2019].

Department of Health & Social Care. 2018. *The future of healthcare: our vision for digital, data and technology in health and care*. Available from: https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care [Accessed 20th October 2018].

Digital Health. 2018. *WhatsApp doc: Legal and practical perspectives of using mobile messaging.* Available from: https://www.digitalhealth.net/2018/02/whatsapp-doc-legal-and-practical-perspectives-of-using-mobile-messaging/ [Accessed 30th July 2019].

Doargajudhur, M., Dell, P. 2018. *The Effect of Bring Your Own Device (BYOD) Adoption on Work Performance and Motivation.* Available from: https://doi.org/10.1080/08874417.2018.1543001 [Accessed 30th July 2019].

Flintshire County Council. 2019. *Bring Your Own Device (BYOD) Policy v2.0.* Obtained via FOI Request by emailing foi@flintshire.gov.uk. Request reference number F0018311.

Fitzgerald, F., Kruschwitz, N., Bonnet, D., Welch, M. 2013. *Embracing digital technology. A new strategic imperative.* Available from: https://sloanreview.mit.edu/projects/embracing-digital-technology/ [Accessed 28th September 2019].

Glaser, B. G., Strauss, A. L. 1967. *The discovery of grounded theory.* Chicago: Aldine Publishing Company.

Goodhue, D. L., Thompson, R. L. 1995. *Task-technology fit and individual performance.* MIS Quarterly, 19(2), 213-236. Available from: https://pdfs.semanticscholar.org/668e/58d4e3479317257a41ce66c688a8aa663399.pdf [Accessed 31st July 2019].

Great Yarmouth And Waveney CCG. 2017. *Bring Your Own Device Policy.* Version 13. Page 5. Section 7.1. Policy obtained via FOI request 001224.

Hallet, J., Aspinall, D. 2017. *Common Concerns in BYOD Policies*. Available from: http://groups.inf.ed.ac.uk/security/appguarden/papers/imps-2017-byod.pdf [Accessed 17th May 2019].

Kanaracus, C. 2013. *Half of companies will require BYOD by 2017.* Available from: https://www.pcworld.com/article/2036980/half-of-companies-will-require-byod-by-2017-gartner-says.html [Accessed 31st July 2019].

Köffer, S., Ortbach, K. C., Niehaves, B. 2014. *Exploring the Relationship between IT Consumerization and Job Performance: A Theoretical Framework for Future Research.* Available from: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=3823&context=cais [Accessed 31st July 2019].

Lee, D. 2019. *WhatsApp discovers 'targeted' surveillance attack.* Available from: https://www.bbc.co.uk/news/technology-48262681 [Accessed 30th July 2019].

Leventhal, R. 2017. Nurses, *Physicians Use Personal Devices Even When BYOD is Prohibited.* Available from: https://www.hcinnovationgroup.com/cybersecurity/news/13029187/nurses-physicians-use-personal-devices-even-when-byod-is-prohibited [Accessed 30th July 2019].

Lincoln, Y.S., Guba, E. G. 1985. *Naturalistic Inquiry*. Thousand Oaks, CA. Sage. p 202. Available to loan from: https://archive.org. [Accessed 29/08/2019].

Mahindru, R. 2013. *Bring your own device (BYOD): An empirical study across industries.* Available from: https://ijrcm.org.in/article_info.php?article_id=4095 [Accessed 17th May 2019].

Meske, C., Stieglitz, S., Brockmann, T., Ross, B. 2017. *Impact of Mobile IT Consumerization on Organizations – An Empirical Study on the Adoption of BYOD Practices.* Available from: https://link-springer-com.iclibezp1.cc.ic.ac.uk/content/pdf/10.1007%2F978-3-319-58484-3_27.pdf [Accessed 17th May 2019].

Merriam, S. B., & Tisdell, E. J. 2016. *Qualitative research: a guide to design and implementation.* San Francisco, CA . John Wiley & Sons.

Mitrovic, Z., Veljkovic, I., Whyte, G., Thompson, K. 2014. *Introducing BYOD in an organisation: the risk and customer services viewpoints.* Available from: https://www.researchgate.net/publication/267642925_Introducing_BYOD_in_an_organisation_the_risk_and_customer_services_viewpoints [Accessed 2nd August 2019].

National Cyber Security Centre. 2016. *BYOD: Executive Summary*. Available from: https://www.ncsc.gov.uk/guidance/byod-executive-summary [Accessed 18th September 2019].

NHS Digital. 2019. *Internet First.* Available from: https://digital.nhs.uk/services/internet-first [Accessed 30th July 2019].

NHS Digital. 2017a. *BYOD security example policy*. Available from: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/k/byod_security_-_example_policy_230517.pdf [Accessed 15th July 2019].

NHS Digital. 2017b. *Acceptable use example policy.* Available from: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/0/7/acceptable_use_-_example_policy_230517.pdf [Accessed 15th July 2019].

NHS England. 2019a. *The NHS Long Term Plan.* Available from: https://www.longtermplan.nhs.uk [Accessed 15th July 2019].

NHS England. 2019b. *Securing Excellence in Primary Care (GP) Digital Services: The Primary Care GP Digital Services Operating Model 2019-21.* Page 131. Available from: https://www.england.nhs.uk/publication/securing-excellence-in-primary-care-gp-digital-services-the-primary-care-gp-digital-services-operating-model-2019-21/ [Accessed 27th January 2020].

NHS England. 2019c. *Acceptable Use Policy excerpt relating to BYOD.* Policy obtained via FOI request FOI-1911-1103768.

Oaks, J. 2013. *Why BYOD is Good for People, Planet and Profit.* Available from: https://www.triplepundit.com/story/2013/why-byod-good-people-planet-and-profit/47456 [Accessed 14th December 2019].

Ofcom. 2018. *A decade of digital dependency.* Available from: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2018/decade-of-digital-dependency [Accessed 27th January 2020].

Oppenheim, A.N. 1992. *Questionnaire design, interviewing and attitude measurement.* Continuum, London.

Pagliari, C. 2007. *Design and Evaluation in eHealth: Challenges and Implications for an Interdisciplinary Field.* Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1913937/ [Accessed 17th May 2019].

Patton, M. Q., 2015. *Qualitative research and evaluation methods (4th ed.).* Thousand Oaks, CA. Sage.

Royal Marsden NHS FT. 2019. *IT Acceptable Use Policy.* Version 1. Page 8. Section 4.2.1. Policy obtained via FOI request 4479.

Somerset Partnership NHS FT. 2015. *Information Security Policy.* Version 6. Page 22. Section E1. Policy obtained via FOI request Q3 19 45.

Stephens, K., Zhu, Y., Harrison, M., Iyer, M., Hairston, T., Luk, J. 2017. *Bring Your Own Mobile Device (BYOD) to the Hospital: Layered Boundary Barriers and Divergent Boundary Management Strategies* Available from: http://hdl.handle.net/10125/41584 [Accessed 17th May 2019].

The Information Commissioners Office. 2019. *Bring your own device (BYOD).* Available from: https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf [Accessed 18th September 2019].

Varbanov, R., 2014. *Applications of the BYOD conception – benefits, risks and approaches.* Available from: https://econpapers.repec.org/article/datbmngmt/y_3a2014_3ai_3a2_3ap_3a12.htm [Accessed 17th May 2019].

Weeger, A., Wang, X, Gerald, H. 2015. *IT Consumerization BYOD Program Acceptance and its Impact on Employer Attractiveness.* Available from: https://www.tandfonline.com/doi/pdf/10.1080/08874417.2015.11645795 [Accessed 17th May 2019].

Westerman, G., Bonnet, D., McAfee, A. 2014. *Leading Digital Change.* Harvard Business Review Press, Boston, Massachusetts. p 156, 174.

Williams, J. 2014. *Left to their own devices: How healthcare organizations are tackling the BYOD trend.* Biomedical Instrumentation and Technology. 48 (5) (pp 327-339), 2014. Date of Publication: 01 Sep 2014. Available from: https://www.aami-bit.org/doi/pdf/10.2345/0899-8205-48.5.327 [Accessed 24th May 2019].

Definitions

Bring Your Own Device (BYOD): A policy (with associated organisational procedures and methods) to allow employees to utilise personally owned devices (laptops, tablets, and smartphones) in their workplace, and to use those devices to securely access organisations' systems, applications and information.

Choose Your Own Device (CYOD): A policy (with associated organisational procedures and methods) to allow employees to select their preference from a choice of devices (laptops, tablets, and smartphones) provided by their organisation for use in the workplace.

Freedom of Information (FOI) Request: The process of requesting information via The Freedom of Information Act 2000 which enables every UK citizen the right to request information held by the public bodies and organisations, including the government, regulators and any public service companies, such as the BBC.

Integrated Care System (ICS): A regional partnership of NHS organisations, local councils and others who take collective responsibility for managing resources, delivering NHS standards, and improving the health of the population they serve.

Internet of Things (IoT): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. Examples could include smart watches, smart lights and internet connected speakers.

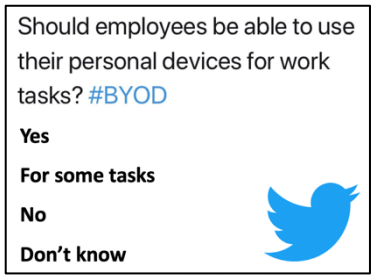
Mobile Device Management (MDM): Software which allows the management and control of smartphones, tablets and computer devices enabling access to organisations' systems and data in a way that protects the data and the corporate network. MDM enables restrictions to be enforced via identity on user devices and provides the ability to remove data and apps or completely wipe devices remotely should the need arise.

Personal Identifiable Data (PID): Any information that is personal and would identify you as an individual such as name, date of birth, address, NHS number.

APPENDIX A - User survey questions

Twitter Poll question

(https://twitter.com/robblagden/status/1166817053073956866)



User Survey Questions

(https://www.surveymonkey.co.uk/r/BYOD_Survey)

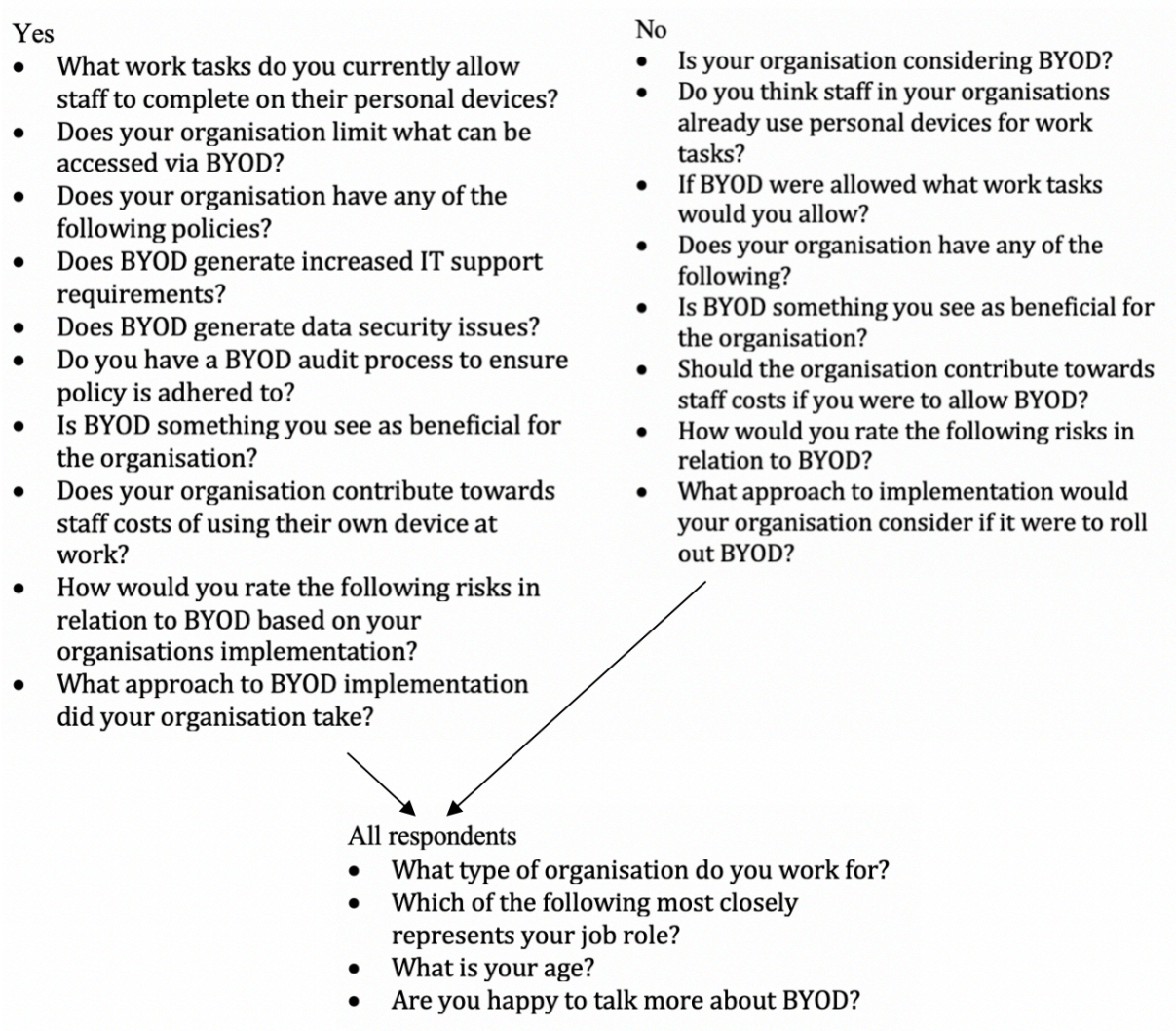
- What is your first reaction to Bring Your Own Device?
- Do you already do work tasks on your own device?
- If BYOD were allowed what work tasks would you find useful to do on your own device?
- How do you feel about using your own device for work tasks?
- Thinking about Bring Your Own Device, is it something you see as beneficial?
- Should the organisation contribute towards costs if you were to use your own device at work?
- If Bring Your Own Device were available today, how likely would you be to sign up?
- What type of organisation do you work for?
- Which of the following most closely represents your job role?
- When did you qualify for your role?
- What is your age?
- Are you happy to talk more about BYOD?

APPENDIX B - Technical survey questions and pathway

Technical Survey

ps://www.surveymonkey.co.uk/r/BYOD_TechSurvey)

Does your organisation have a Bring Your Own Device policy or allow use of personal devices for work use?



APPENDIX C – Public sector FOI questions

FOI Email Template

Dear [FOI Organisation Name],

I am pursuing a Masters degree in Digital Health Leadership at Imperial College London and am conducting a research study for my dissertation.
My study aims to examine how to improve the implementation of Bring Your Own Device (BYOD) in the public sector.

I am writing to you under the Freedom of Information Act 2000 to request the following information:

1. Does [FOI Organisation Name] allow staff to use their own devices to access work email? Please answer Yes or No.
2. Does [FOI Organisation Name] allow staff to use their own devices for any other work-related activities? Please answer Yes or No.
3. If you answered yes to question 2 please provide a list of the types of systems that staff can access from personally owned devices?
4. Does [FOI Organisation Name] have a policy that covers BYOD or the use of personal devices at work? Please answer Yes or No.
5. If you answered yes to question 4 please could you provide a copy of your policy that covers BYOD or personal device usage at work?

If you have any queries please don't hesitate to contact me via email and I will be very happy to clarify what I am asking for and discuss the request, my details are outlined below.

Thank you for your time and I look forward to your response.

Best wishes,

Rob Blagden
robert.blagden18@imperial.ac.uk

APPENDIX D – Interview Questions

Interview Questions for Users

#	Question	Question Type (Patton, 2015)
1	How did you find the survey when you completed it?	Opinion & values Experience & Behaviour
2	In what ways to you currently use BYOD at work (if any)?	Knowledge Experience & Behaviour
3	If you could use your own device more at work how would this change your typical day?	Hypothetical
4	How would you feel about these changes caused by BYOD?	Feeling
5	What benefits could there be of BYOD in your job role?	Opinion & values Experience & Behaviour
6	Can you think of any challenges BYOD may cause for you or your organisation?	Knowledge Opinion & values
7	What are your thoughts about downsides to BYOD?	Opinion & values
8	What do you feel about accessing patient data on your personal phone?	Feeling
9	If the technical team could provide assurance data would be safe would this make you more comfortable with BYOD?	Opinion & values
10	Do you think BYOD would impact work life balance? Why?	Opinion & values Feeling

Interview Questions for Technical staff who have implemented BYOD

#	Question	Question Type (Patton, 2015)
1	How long has your organisation operated BYOD?	Knowledge
2	What was your approach to implementation? Any software products in use? Any limitations	Experience & Behaviour
3	What can and can't users do? What type of devices are supported? Do you offer BYOD to all staff?	Knowledge
4	What have been the biggest challenges?	Experience & Behaviour
5	What have been the benefits?	Opinion & values
6	Do you feel BYOD has been a success for your organisation?	Feeling, Opinion & values
7	What has the response been like from users?	Opinion & values
8	How well do users maintain their devices and keep the OS and Apps updated?	Knowledge
9	What is your approach to audit?	Experience & Behaviour
10	Have you had any data breaches or issues because of BYOD?	Experience & Behaviour
11	Do you feel access and equality is effectively managed in relation to BYOD?	Feeling, Opinion & values
12	What differences have your seen in approaches to work because of BYOD?	Experience & Behaviour
13	What impact on IT operating costs has BYOD caused?	Knowledge
14	If you needed to implement BYOD again in the future what would you do differently?	Hypothetical
15	Do you have a BYOD policy? Can I have a copy?	Knowledge

Interview Questions for Technical staff who do not use BYOD

#	**Question**	**Question Type (Patton, 2015)**
1	When will your organisation roll out BYOD?	Knowledge
2	How will you approach implementation? Phased rollout / big bang?	Experience & Behaviour Knowledge Possibly Hypothetical
3	Do you think there will be any barriers to roll out?	Knowledge Opinion & values
4	Will you offer BYOD to all staff?	Knowledge
5	If no plans for BYOD how many of your users already use messaging and email on personal devices and how to you manage this?	Knowledge Experience & Behaviour
6	What do you feel are the benefits of BYOD?	Feeling
7	What challenges do you think BYOD will bring?	Opinion & values
8	Are your users asking for BYOD?	Experience & Behaviour Opinion & values
9	How will you approach BYOD audit?	Knowledge Experience & Behaviour
10	How will you manage equality in relation to BYOD?	Opinion & values Experience & Behaviour
11	Were there any thoughts or concerns you wanted to share?	Any or all.
12	Do you have a BYOD policy yet? Can I have a copy?	Knowledge

APPENDIX E – Example BYOD policy

This example policy has been developed as guidance for organisations as a result of this research study. It purposely uses simple non-technical language to ensure it is readable and provides clear instructions for users.

Bring Your Own Device (BYOD) Policy

Example Policy for Healthcare

Author	: 01568418
Version	: 1.0
Date Created	: 08/03/2020
Date Approved	:
Approved By	:
Review Required	: March 2022

1. Introduction

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, tablets or laptops) in the workplace, and to use those devices to securely access the organisation's systems, applications and information.

BYOD is optional and offered to provide greater flexibility. It may not be available to all staff.

This policy provides guidance which must be followed when using your own device at work. All users of BYOD are required to read this policy in full and confirm they understand and will comply with it. A summary of important points is provided below.

Do

- ✓ **Keep your passwords secure**
- ✓ **Use biometric features to secure the device if possible**
- ✓ **Keep your operating system updated**
- ✓ **Be careful who can see your screen when accessing work systems**
- ✓ **Report lost or stolen devices**
- ✓ **Be aware of your responsibility for all costs**
- ✓ **Allow IT to conduct spot checks if required**
- ✓ **Inform IT if you leave employment with the organisation**

Don't

- ✘ **Don't share your device or passwords**
- ✘ **Don't use BYOD when you are not working**
- ✘ **Don't make copies of data or take screenshots**
- ✘ **Don't access systems without authorisation**
- ✘ **Don't save work in unapproved locations or applications**

2. Scope

This policy applies to all staff and authorised third parties of the organisation who voluntarily choose to use BYOD.

The BYOD service includes a range of systems and access may vary by individual depending on the requirements of individual roles.

Available systems include:

- Email
- Calendar
- Intranet & web browsing
- Internal web-based systems
- Rota/scheduling
- Communication systems
- Reporting systems
- Clinical systems

3. Aims

To ensure BYOD systems and data are used appropriately, legally and securely.

To ensure personally owned devices are used in a manner which protects confidentiality in accordance with GDPR.

To ensure staff clearly understand their responsibilities when using BYOD.

4. Supported Devices

Due to the rapid pace of change it is not possible to support BYOD on all devices.
BYOD will only be supported on devices which will run the latest version of the Apple or Android operating system. Staff will be expected to ensure devices are kept updated or risk losing access to some systems.

Devices must be encrypted and have passcode or biometric security if available with a timeout to lock automatically after 5 minutes of inactivity. Jailbroken or rooted devices are strictly prohibited. Staff must not circumvent security controls.

The organisation's BYOD software must be installed on devices in order for access to be granted to systems. Staff must not remove or modify the BYOD software on their device.

Technical support will be limited to the organisation's BYOD software and systems.
Connectivity via WiFi or mobile data contracts will be the responsibility of the device owner.

5. Access

Devices may connect over Guest / NHS WiFi but are not permitted to connect directly to the corporate network.

Use of BYOD and access to corporate systems is subject to other organisation policies and practices and does not override or supersede them.

BYOD is optional and may not be appropriate in all roles.
The organisation reserves the right to revoke access if staff do not follow this policy.

6. Responsibilities

Staff may only connect to organisation systems for the purpose of authorised work.

Use of a device that has access to work systems via BYOD should be limited to its owner and must not be shared. Devices must be maintained as stated in section 4.

Account logon, passwords and pins must be kept confidential and never shared with others. Staff should be conscious of the setting in which devices are being operated and should ensure data and systems displayed are not visible to others. Data accessed must not be saved to the device or copied off it. Screenshots of systems must not be taken.

Staff must inform IT if they leave employment with the organisation.

Staff must comply with all relevant legislation including not using BYOD whilst driving.

Staff must read and understand and adhere to other key policies including:

- IT Acceptable Use Policy
- IT Security Policy
- Mobile Working Policy

Staff must immediately inform IT if:

- Your password has been breached
- Your device gets lost or stolen
- Organisational systems are not working normally

7. Loss or Damage

The organisation will not accept any liability for loss or damage of personal devices and data that are using the BYOD system.

Staff should inform IT immediately if they lose their personal device or have It stolen. IT will attempt to remotely wipe or disable the device.

8. Acceptable Use

Staff should only use BYOD to access work systems during working hours.

Staff should only access systems which they require and normally use.

Staff should never try to access systems for which they are not authorised.

Confidential data should only be accessed for a specific work-related requirement.

Any suspected breach must be immediately reported to IT.

9. Costs

Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.

Staff are responsible for all mobile data or WiFi hotspot costs related to BYOD usage and should monitor these to ensure they have sufficient allowance.

10. Monitoring

The organisation will monitor usage BYOD devices from time to time including the make and model of devices in use and the version of the operating system currently installed. Where operating systems are found to be out of date the staff member will be informed and expected to upgrade to the most current version within 5 days.
Failure to remediate will result in access to BYOD services being withdrawn.

Spot checks on BYOD devices may be initiated at any time and staff will be expected to allow access to authorised personnel to check settings related to BYOD usage. Spot checks will always be conducted in the presence of the staff member and devices will never be taken away from their owner.

Technical support personnel can access details on usage of corporate applications via the BYOD system but cannot access personal application data. In some instances, device location may be collected but this data will only be used if the device is lost or stolen.

11. Digital Equity

The organisation is committed to digital equity. All systems accessible via BYOD are also available via the corporate network and computer system.

Where there is a genuine business need for a mobile device, and BYOD is not the staff members preferred option, the organisation will provide suitable device.

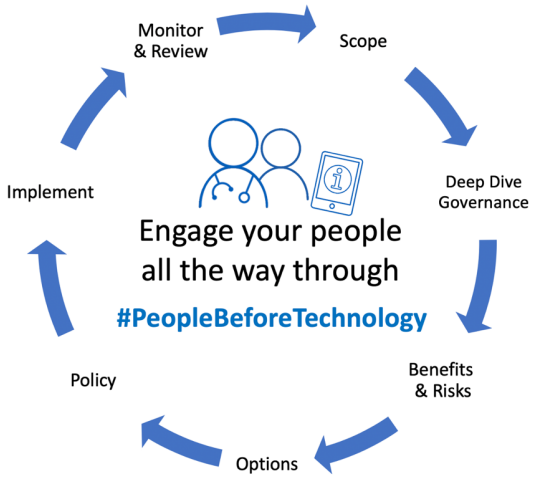
APPENDIX F – BYOD implementation guide for healthcare

This implementation guide has been developed as a way to disseminate findings of this study to organisations who may be considering rollout of BYOD.

Bring Your Own Device (BYOD) Guide

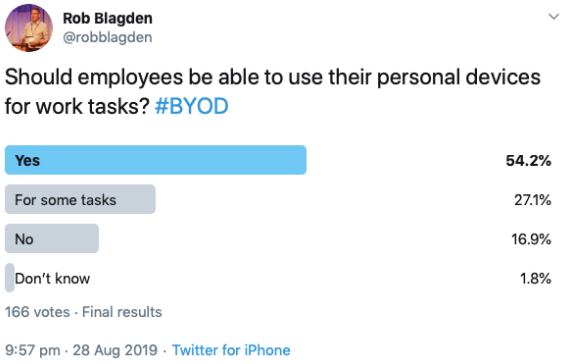
Implementation Guide for Healthcare

Author : 01568418
Version : 1.0
Date Created : 08/03/2020



Introduction

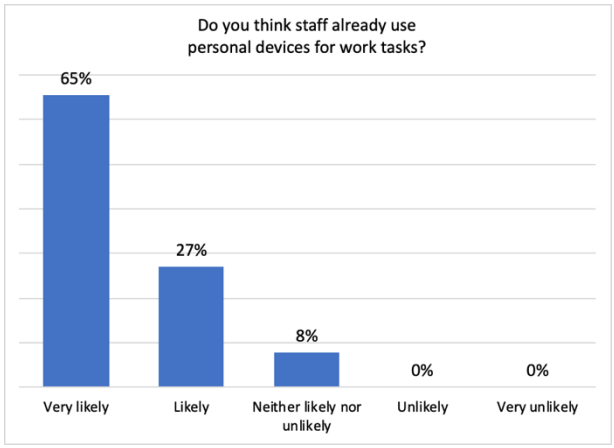
BYOD is used across the globe to offer flexible working arrangements for employees and there is evidence which shows it can improve innovation, efficiency and morale. There is a strong desire in the workforce to have choice in whether they use their own device for work tasks. Organisations can potentially benefit from a more engaged and productive workforce whilst helping to manage down technology costs. There are sustainability advantages from using BYOD reducing the environmental impact of raw material and power consumption.

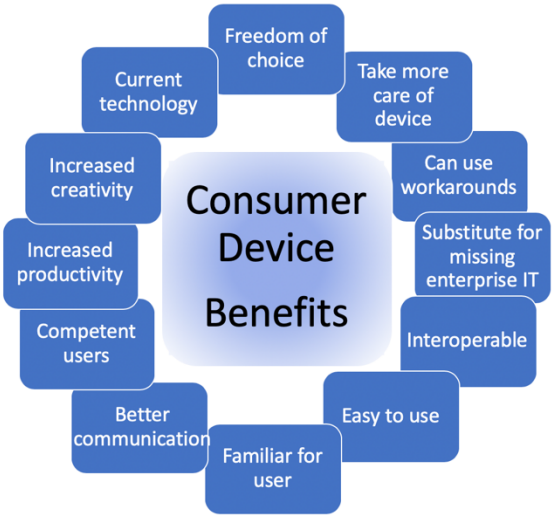


In a 2019 Twitter survey there was an overwhelming desire from employees for BYOD.

Over 80% of respondents said they wanted to use their own device for at least some work tasks.

In another survey 92% of organisations, not offering BYOD, said it was likely or very likely that staff were already using personal devices in the workplace regardless of policy.





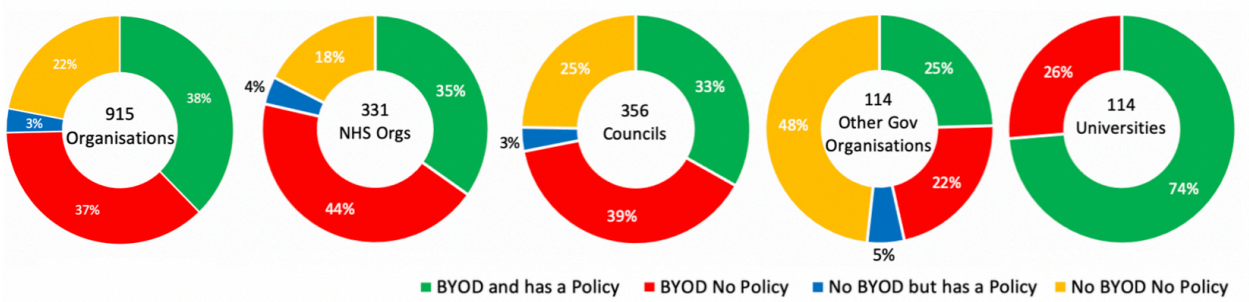
81% of the organisations surveyed thought BYOD was definitely or probably beneficial.

BYOD offers a wide range benefits for both the employee and the organisation.

But…the NHS has a range of unique challenges that require special focus above and beyond the needs of other organisations.

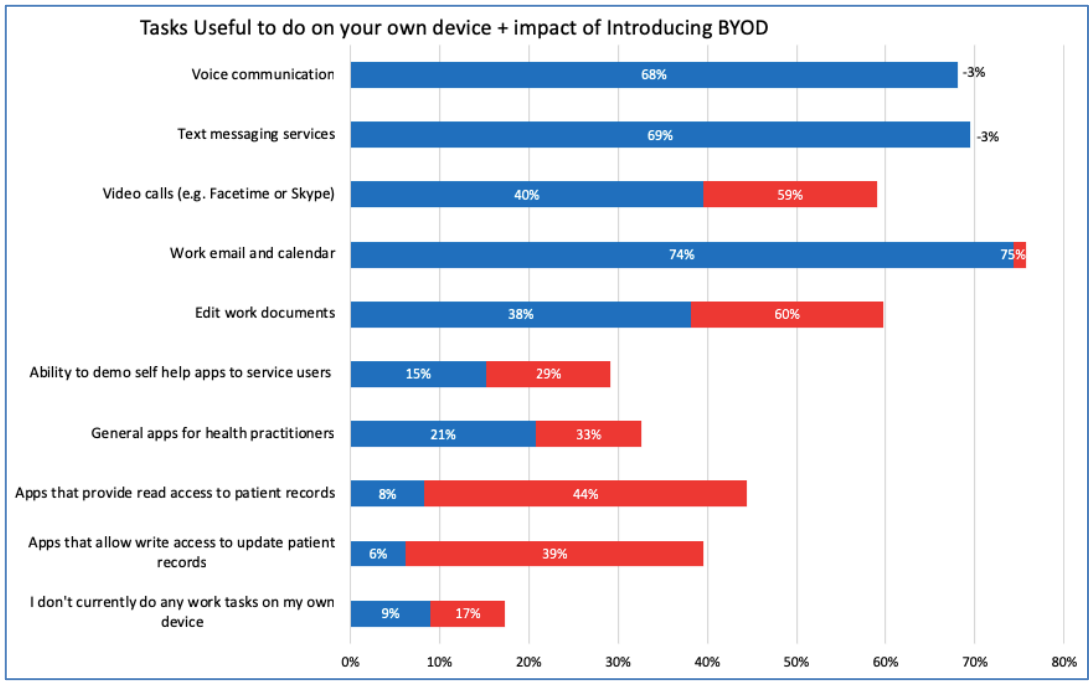
For instance:

- Does the value of patient data alter how BYOD is secured in the NHS?
- How will clinicians maintain a healthy work/life balance if their personal smartphone also provides intrusive alerts on the condition of their patients when off-duty?
- Is there benefit from BYOD if the most useful data lives in legacy systems which limit accessibility and flexibility?
- How can a standard approach be used when the knowledge and risk appetite in each NHS organisation is far from standard?
- In large NHS organisations with a range of roles and systems how do you ensure solutions maintain digital equity and avoid digital division?



A key discovery in a recent study revealed 37% of organisations offering BYOD don't have policies. In the NHS this rose to 44%. Often where policies are provided, they are confusing and difficult for employees to access. Where policies do exist only 36% of those surveyed said they had an audit or monitoring process.

Organisations did believe there were benefits in offering BYOD and the survey data revealed a likely uptake in a number of key areas shown below. Blue areas are usage reported today and the red areas indicate uptake if BYOD were available.



There is no single implementation methodology for BYOD in the NHS because every organisation is different. Size, culture, ambition and leadership will all influence your specific implementation journey. Keeping BYOD optional is important but so too is maintaining equity and avoiding a digital divide.

This guide is the result of a yearlong study into BYOD in the NHS. It is not a set of instructions on how to safely and successfully roll out BYOD, rather it presents a list of suggestions and questions you might want to consider to help your project.

It is hoped the information provided will inform the BYOD approach that is right for your organisation.

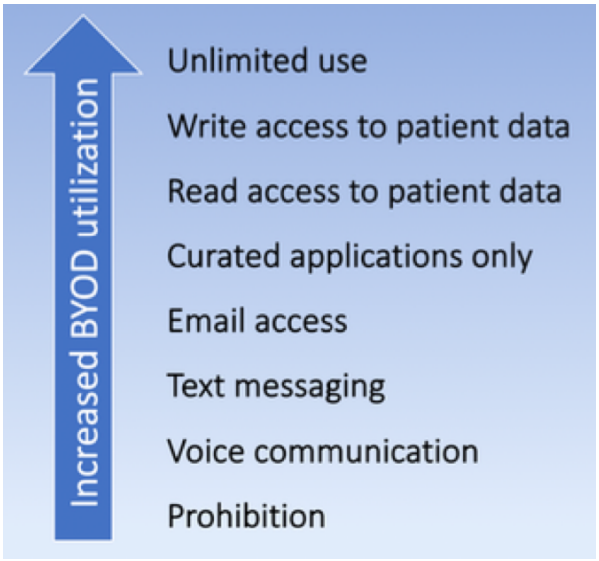
1. Engage colleagues all the way through

In every project, but especially technology projects, people are the most critical aspect. The human interface between electronic systems and real-world processes is often where unexpected outcomes can occur and maintaining an open dialog is essential to success. The engagement suggestions below are not exhaustive so find the methods that work for you. Many projects have failed due to a lack of engagement, use techniques at the start of your project but also at every stage of your project to ensure people are connected with what you are doing.

- Use workshops throughout to gather views and be willing to accept there will be differences of opinion.
- Work closely with staff to review how BYOD could be beneficial for the colleagues, the organisation and service users.
- Consult staff on ways they already benefit from using their own device.
- Have impartial experts available to provide guidance and advice to support the conversation.
- Listen to staff perspectives on the safety of patient data and the concerns about the potential impact to work/life balance.
- Clinicians need assurance the organisation won't proceed to offer clinical system access via BYOD on day one without adequate controls, their input and confidence needs to be highly valued.
- Gather a list of the areas where there is agreement BYOD could add value.
- Dig deeper into the areas of consensus and discuss the impact and risks openly and honestly.
- Form a group to take the project forward and include clinicians, IG leads, those with the biggest concerns, board members and keen early adopters.
- Board leadership and support is key in a digital transformation project.

2. Develop your scope

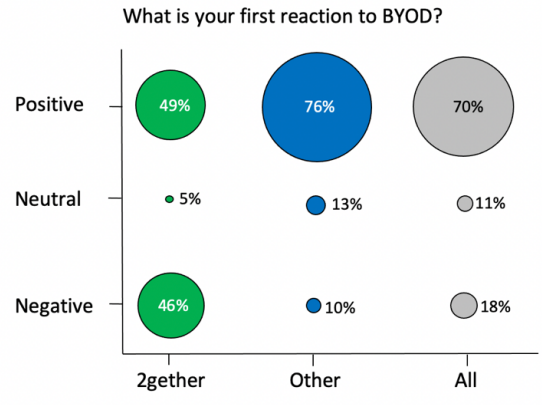
There are a range of levels to which you can implement BYOD, it doesn't have to be an all or nothing approach. Scaling up over time by starting with low risk but high benefit apps will build trust in BYOD. Building confidence in systems is just as important for technical teams as it is for others.



- Agree on the initial objectives and outcomes.
- What are the specific use cases? Initially perhaps these will be business applications with wide appeal rather than clinical. Also consider applications which will make a difference to clinicians; perhaps rotas, secure messaging apps or reference data to support clinical practice.
- Who will your users be and are they interested in BYOD solutions?
- If you don't offer email or calendar these could be good starter BYOD applications because they have wide appeal. Having access to a calendar on the move can be really useful and doesn't require users to have the latest or best smartphone device.
- Talk with other similar organisations who already use BYOD about where they have seen the maximum benefit.
- Are there areas of weakness that BYOD could help you address? For instance, there is evidence BYOD can increase employee satisfaction, productivity and innovation. There are studies which have proven a link between employee retention and BYOD. Could BYOD be a differentiator for your organisation in some form?
- Once decided think about total number of users that could utilise the solution and who might form a subset to engage in a pilot to test solutions and assumptions.

3. Deep dive governance

Setting up appropriate governance for your BYOD implementation is essential. In research it was found that clinical staff had significant concerns about BYOD in terms of data security and being free from intrusive alerts when not at work. Reviewing processes will help address these concerns.



In a survey question asking for people's reaction to BYOD the feedback was generally positive, although the focus organisation's response was mixed because of clinician concerns over data security and expectations the organisation may place on them.

Here are some steps to help you think about system and data governance:

- Review the planned scope and break down in detail exactly what data will be required, where it exists today and how it will be managed.
- Limit data to what is required to enable the anticipated outcome.
- Classify the types of information and have clarity on whether any is confidential or personal identifiable data (PID) and who currently owns it.
- Think about how data will be transferred, accessed and stored on devices.
- Prioritise presenting/streaming data to BYOD rather than storing data on devices.
- Be clear where the data ownership responsibility applies regardless of processing device.
- Think about how you will protect staff from alerts when they are not at work.
- Start documenting top tips for users and continue to build them throughout the project.
- Consider requirements for the NHS Data Security and Protection Toolkit from the start to ensure you design compliant processes.
- Review ICO best practice for BYOD implementations.
- Review National Cyber Security Centre BYOD advice.

4. Analyse benefits and risks

You've thought about what you might offer via BYOD and the data involved, next you need to review the benefits you'll get and analyse the risks. Baselining these and selecting KPIs will help you measure success once your project completes.

Benefits

- Baseline the current process and future benefits of the BYOD approach.
- Are there time, quality and cost benefits involved? BYOD has been linked to productivity gains, employee satisfaction, morale improvements, increased innovation and flexibility, employee retention and more.
- Think about how you can measure these potential benefits now and in the future.

Risks

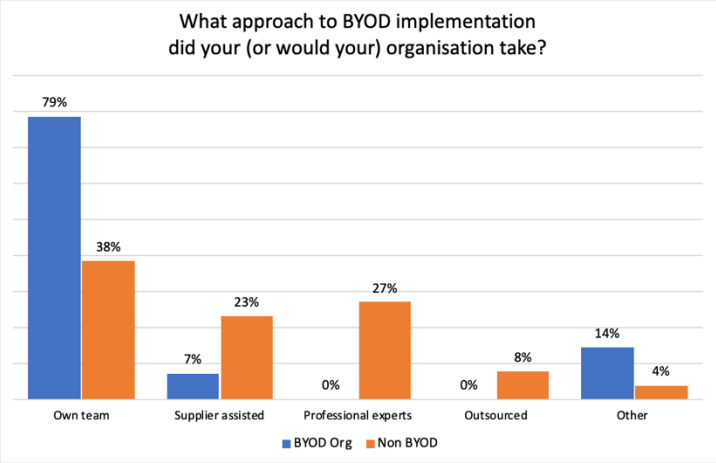
- What are the risks involved in the proposed application of BYOD?
- Perceptions and opportunity may differ between roles impacting uptake and use of BYOD.
- Consider security risks, adoption barriers, knowledge and training challenges, costs to implement and those of ongoing administration and management.
- Review options to mitigate and manage the risks documented.

KPIs

- Identify your primary reason for implementing BYOD and decide on some key performance indicators which will help you monitor progress towards this goal.
- Useful metrics might be:
    - Number of Users / Logons / Minutes of use
    - Productivity feedback from users
    - Employee satisfaction
    - Helpdesk support impact / IT costs
    - Staff retention over time

5. Investigate technical options

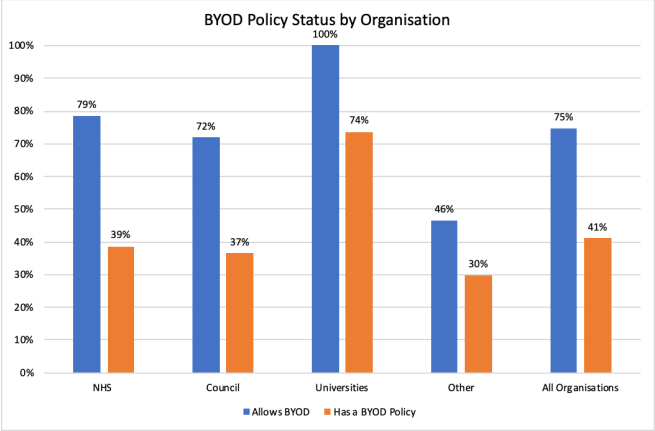
Research revealed a difference in perspective on how BYOD should be implemented.



Those who had implemented BYOD mostly did it within their own teams whilst those thinking about BYOD were more varied about the best route to implement. The impact on IT support was minimal in BYOD organisations whereas to those yet to implement said it was their highest concern.

- Work with local organisations and those in a similar sector to yourself who have already successfully implemented BYOD. Don't reinvent the wheel.
- Understand challenges faced by other organisations and heed their lessons learnt.
- Many existing NHS BYOD organisations implemented with their own staff which brings local knowledge of the trust's existing systems, policies and culture.
- Also consider external support to bring in new ideas and help the project avoid blind spots caused by policy legacy or a lack of experience.
- Large scale rollouts have succeeded in having a low support impact and focusing on this will make the solution sustainable and cost effective.
- Look for technical systems which will provide the required controls. Most Mobile Device Management (MDM) solutions can be configured to protect data and devices without impacting personal user data. Investigate the market and test assumptions.
- Model the costs of various options and the potential savings.
- Visit organisations using different products to understand how they work in context.
- Aim to containerise BYOD apps for your employees to separate work apps from personal.
- Consider using a curated app store and ensure there is a process for employees to request updates to the list of trusted software.

6. Build policy and processes



Now you've determined your technical solution and data governance and you know the risks to avoid and the benefits you desire you're set to develop your policy and processes. Research revealed that many organisations operate BYOD without any policy. Where policies were in place, often they were hard to find and difficult to understand.

Write your policy with the reader in mind. An example policy is provided alongside this guide.

- Develop a new stand-alone BYOD policy so staff know where to find the latest guidance.
- Be clear about the responsibilities on the user to maintain their device security.
- Don't make BYOD mandatory but offer it as widely as possible.
- Assure staff about how BYOD systems are secured and what personal data might be accessible to the employer.
- Ensure the policy covers audit processes to monitor and review BYOD compliance.
- Address the issue of remuneration so that employees are clear where they stand on costs.
- Consider what happens if personal devices get damaged during work usage.
- Build a culture of trust and encourage staff to self-report issues to enable rapid resolution.
- Build processes for onboarding and offboarding of users.
- Ensure a process exists to allow staff to request apps be added to the curated app store.
- Review other policies which may reference the use of personal devices, update them to reflect the organisations BYOD approach.
- Consider whether multi-level policies would be beneficial if usage of BYOD or application access could be different based on role or position.
- Update the standard IT change control processes to always consider impact on BYOD systems.

7. Implement

Implementation of a BYOD solution is similar to any project although there are two key areas to be aware of. Firstly, you are probably providing access to an application via a new route and this needs thorough planning and testing. Secondly, you are offering a completely new way of working to users and should recognise and respect the cultural norms you may be disrupting.

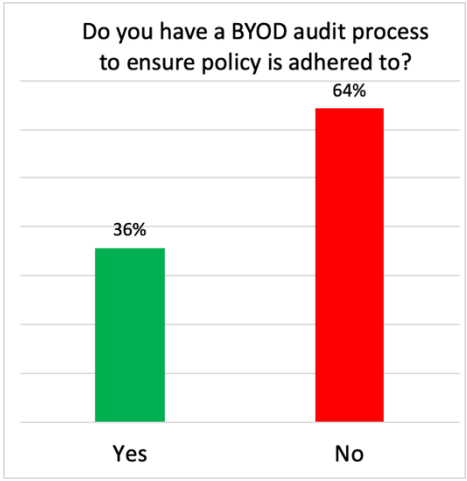
- Develop an implementation plan and consider including the following:
    - Documentation and objectives from your work so far
    - Lots of user engagement and comms
    - Procurement and solution options
    - Implementation phases and test plans
    - Technical assurance via external penetration testing
    - User training and support plan

- Rollout the chosen solution carefully and ensure comprehensive testing throughout.
- Review WiFi and network capacity where there could be high utilisation of BYOD.
- Provide training to colleagues as the solution is launched ensuring expectations are explicitly discussed such as the user need to maintain the device's software and to report any problems.
- Roll out to support staff first so that they can familiarise themselves with how the solution works.
- Check the documentation for users and support staff is adequate.
- Work closely with colleagues to resolve issues as they occur.
- Keep your organisation updated on the plans and the progress.
- Monitor impact on work / life balance, be sure to protect staff from overwork.
- Consider how systems would be shut down or devices wiped if there were a need.

8. Monitor and review

Many organisations don't have a BYOD policy and even those who do often don't have a process to monitor and review compliance.

Given the concerns about data security and the potential for additional pressure on some individuals it is essential that some form of monitoring is put in place.



- Audit for compliance regularly throughout rollout and follow up on audit outcomes.
- Review benchmarks and KPIs pre and post implementation and on an ongoing basis.
- Conduct a systematic review of the project – use interviews and surveys to gain insight into how productivity and/or staff morale have been impacted.
- Identify the actual benefits and costs.
- What issues were uncovered and how were they addressed?
- What was the support impact?
- Update documentation, processes and policy at least annually.
- Remember your systems and user devices continually evolve.
- Report progress and decide to scale up if all goes to plan.
- Think about another application or use-case.